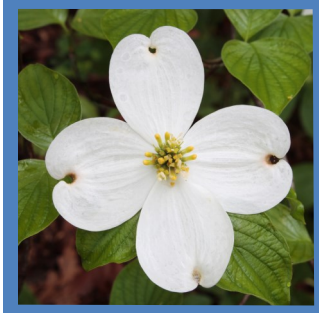

AGENCIES OF THE SECRETARY OF HEALTH AND HUMAN RESOURCES

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2019

Auditor of Public Accounts
Martha S. Mavredes, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

This report summarizes our fiscal year 2019 audit results for the following four agencies under the Secretary of Health and Human Resources. Collectively, these four agencies spent $15.8 billion or 96 percent of the total expenses for agencies under this secretariat.

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

Our audits of these agencies arise from our work on the Commonwealth's Comprehensive Annual Financial Report and Statewide Single Audit of federal funds. Overall, we found the following:

- proper recording and reporting of all transactions, in all material respects, in the Commonwealth's accounting and financial reporting system, each agency's accounting records, and other financial information reported to the Department of Accounts;

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

- 43 of the 61 findings are also considered to be instances of non-compliance with applicable laws and regulations that are required to be reported; and

- 30 of the 61 findings are matters not adequately resolved from the previous year that are repeated in this report. Five of these are partial repeats meaning that some progress had been made since our previous report.

Our report also includes a Risk Alert and a Comment to Management, both of which are applicable to the Department of Behavioral Health and Developmental Services.

–TABLE OF CONTENTS–

RISK ALERT

What is a Risk Alert?

During the course of our audit, we encountered an issue that is beyond the corrective action of the Department of Behavioral Health and Developmental Services (DBHDS) management alone and requires the action and cooperation of management, the General Assembly, the Secretary, and the Governor. The following issue represents such a risk to DBHDS and the Commonwealth.

Continue to Comply with the Department of Justice Settlement Agreement

Repeat: Yes (last issued in fiscal year 2016)

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

The Commonwealth continues to work with DOJ and an independent reviewer to meet the terms of the settlement agreement. Under the agreement, full compliance is expected to be demonstrated by June 30, 2020, in order to sustain a full year of compliance to exit court oversight of the agreement in 2021. DBHDS is in the process of negotiating compliance indicators with DOJ in order to specify exactly what the Commonwealth must do to achieve compliance. A court hearing is being held regarding unresolved compliance indicators, and it is expected the court will impose compliance indicators that will require additional resources for the Commonwealth to meet. These compliance indicators will increase reporting requirements and create a need for data quality systems to comply with negotiated metrics. There is a risk of non-compliance if DBHDS does not receive adequate funding at the appropriate time for personnel, information technology resources, and other resources necessary to implement the compliance indicators. Loss or reduction in funding could extend the time that it takes for DBHDS and the Department of Medical Assistance Services (Medical Assistance Services) to implement programs and reach the requirements of the DOJ settlement agreement. Specifically, funds are needed to:

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

- support facility transition waiver slots to enable DBHDS to continue moving individuals out of the training centers and children out of nursing homes and

intermediate care facilities and into community-based services as well as additional community intellectual and developmental disability waiver slots to help reduce the growing waiting list for services;

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

- establish a functioning quality management system.

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

COMMENT TO MANAGEMENT

What is a Comment to Management?

During the course of our audit, we became aware of situations that impact DBHDS facilities and the Central Office. When these challenges are of such magnitude that it is the root cause of a majority of our findings, we communicate that through a Comment to Management. While agency personnel may also be aware of this situation and are preparing to meet this challenge, we issue this communication to highlight the situation to a broader audience in order to encourage continued progress by agency personnel and to ensure there is visibility into their efforts by senior level management of the entity and the Commonwealth.

Dedicate the Necessary Resources to Exercise Adequate Oversight

Repeat: No

The Central Office does not exercise adequate oversight over the functions and activities of its individual facilities. DBHDS is a highly decentralized agency with 13 facilities located across the Commonwealth. For the most part, the facilities share the same processes and use the same systems in their day to day operations. However, facilities lack standard, uniform policies and procedures. In addition, there appears to be a disconnect between staff at the Central Office and the facilities. Throughout the course of our audit, we identified several weaknesses in controls over system access, payroll, retirement benefits, and general controls at the facilities, which resulted in several findings. Specifically, there were issues at all four of the facilities where we performed detailed fieldwork: Central Virginia Training Center, Eastern State Hospital, Southeastern Virginia Training Center, and Southwestern Virginia Mental Health Institute.

Code of Virginia § 37.2-300 establishes the overall structure of the agency and states that DBHDS is under the supervision and management of the Commissioner. Further, Code of Virginia § 37.2-100 defines a "Facility" as a state hospital or training center operated by DBHDS. The issues, which follow, are a result of several contributing factors. Each of the individual facilities operates independently with limited guidance from the Central Office. The Central Office does not have enough resources to adequately oversee the facilities operations and to create standard policies and procedures for individual facilities use. As a result, there continues to be findings related to the facilities. Specifically, there continues to be weaknesses in controls as noted above. Without adequate resources devoted to the oversight function, it is difficult for DBHDS to ensure the activities, controls, and operations of the facilities are functioning as intended.

DBHDS should work to create standard, uniform policies and procedures for facilities use as the facilities share similar processes. DBHDS should advocate for or identify and dedicate the necessary resources to provide appropriate and adequate oversight over the functions and activities of the individual facilities. The Central Office should collaborate with various stakeholders, including facility personnel and the Office of Internal Audit, to improve upon the standardization of processes across all of the DBHDS facilities. The Central Office should provide adequate direction and resources to the facilities to ensure they have sufficient controls over their activities, controls, and operations.

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

This section is organized by agency and each individual finding reported includes information on the type of finding and the severity classification for the finding. The severity classifications are discussed in more detail in the section titled "Independent Auditor's Report." In addition, those findings that report on issues that were not resolved from our previous audit and are repeated in this report are also designated.

The following table summarizes the number of findings by agency and also by the type of finding, either an internal control finding or an internal control and compliance finding. In addition, the table shows how many of those findings are repeat findings by agency.

Number of Internal Control and Compliance Findings by Agency

	Internal Control (only)	Internal Control and Compliance	Total Number of Findings	Repeat Findings**
DBHDS	10	16	26	9
Health	4	7	11	5
Medical Assistance Services	2	4	6*	4
Social Services	2	16	18*	12
Total	**18**	**43**	**61**	**30**

*Indicates agency had a finding classified as a material weakness; Medical Assistance Services had two material weaknesses, and Social Services had one material weakness

** Includes findings that are partial repeats

Why the APA Audits Information Systems Security

DBHDS collects, manages, and stores significant volumes of personal and financial data within its mission critical systems. Because of the highly sensitive and critical nature of this data, DBHDS management must take all necessary precautions to ensure the integrity and security of the data within its systems. To determine if information technology governance, database security, oversight of sensitive systems, and contingency management were adequate, we compared the practices of DBHDS to those required by the Commonwealth's Information Security Standard (Security Standard), SEC 501.

Dedicate Resources to Support Information Security Program

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

DBHDS has been unable to adequately manage and dedicate the necessary resources to support its sensitive systems according to Commonwealth's standards. DBHDS has 211 sensitive systems between the Central Office and the facilities. This number of sensitive systems requires extensive information technology (IT) resources to ensure compliance with the agency's enterprise security program and the Security Standard.

DBHDS stated there are insufficient IT resources at the Central Office and the facilities to properly manage the systems. As a result, DBHDS continues to have weaknesses in certain areas of their information security program with some weaknesses being repeat management recommendations for four years. Specifically, the lack of software baseline configurations and the lack of IT contingency management documentation are areas of concern.

DBHDS began the Facility Application Inventory Reduction initiative in 2017 to reduce the number of applications across the facilities and improve their IT governance program. However, due to a lack of resources and funding, DBHDS did not make progress with this initiative until recently. DBHDS is currently implementing two IT systems that will replace 20 disparate facility systems, bringing the total number of sensitive systems to 191. DBHDS is also working on an enterprise initiative that has the potential to reduce a significant number of systems across the facilities, but the exact number is not yet known. DBHDS stated it is evaluating the resource levels to support the sensitive systems at the Central Office and will do the same for the facilities and expects to complete this effort in April 2020. DBHDS is also implementing a new governance process to manage the procurement and implementation of IT systems at the Central Office and the facilities. DBHDS has a goal to finalize and begin using the new governance process in the first quarter of fiscal year 2020.

Section 2.4.2 of the Security Standard states agency heads are responsible for ensuring that a sufficient information security program is maintained, documented, and effectively communicated to protect the agency's IT systems. Not having sufficient IT resources to manage the sensitive systems at

the Central Office and the facilities increases the risk that certain controls may not exist resulting in a data breach or unauthorized access to confidential and mission-critical data. If a breach occurs and Health Insurance Portability and Accountability Act (HIPAA) data is stolen, the agency can incur large penalties, as much as $1.5 million.

DBHDS should continue to reduce its sensitive system inventory and complete the evaluation of resources that are necessary to support the sensitive systems at the Central Office and the facilities. DBHDS should develop a plan to obtain or reallocate funding to hire the necessary resources to maintain the inventory of sensitive systems according to the Security Standard and complete the new governance structure to assist the agency with managing IT applications and systems going forward. Completing these recommendations will help DBHDS to remediate weaknesses in its information security program and help ensure the confidentiality, integrity, and availability of DBHDS' sensitive data.

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

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

DBHDS had plans to work with the Virginia Information Technologies Agency (VITA) and the new managed services with multi-sourcing services integrator to obtain cost estimates and develop a plan to address disaster recovery and continuity of operations; however, turnover in the Chief Information Officer and Chief Information Security Officer positions as well as staff turnover are the primary factors for not completing this effort. DBHDS does not have an estimate when they will complete the work to obtain cost estimates and develop current IT COOPs and IT DRPs.

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

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

DBHDS should assign the necessary resources and work with VITA and the multi-sourcing services integrator to remediate the weaknesses in the continuity of operations and disaster recovery processes and ensure the contingency management program meets the minimum requirements in the Security Standard. DBHDS should develop and update the COOPs and DRPs ensuring they are consistent across the facilities and the Central Office. Once the COOPs and DRPs are complete, DBHDS should perform annual tests against them to ensure the Central Office and the facilities can restore mission critical and sensitive systems in a timely manner in the event of an outage or disaster. Doing this will help to ensure DBHDS maintains the confidentiality, integrity, and availability of their mission critical and sensitive systems.

Improve Disaster Recovery for Sensitive Systems
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

DBHDS does not perform certain processes in its disaster recovery plan required by the Security Standard and industry best practices. We identified a weakness in this area and communicated this 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 descriptions of security mechanisms contained within the document.

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

DBHDS should implement the controls discussed in the communication marked FOIAE in accordance with the Security Standard and best practices in a timely manner.

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

DBHDS does not have documented baseline configurations for their sensitive systems' hardware and software requirements. DBHDS is working to reduce the total number of sensitive systems but still has 211 sensitive systems, with some containing HIPAA data, social security numbers, and Personal Health Information data. DBHDS was in the process of implementing software that has the ability to establish, configure, and monitor baseline configurations, but the resource implementing it left the agency in September 2018. The agency assigned the work effort to another IT security analyst and planned to complete the implementation in 2019, but due to turnover and competing priorities, DBHDS did not implement the software and there is no estimate when they will complete it.

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

- Develop, document, and maintain a current baseline configuration for information systems. (CM-2)

- Review and update the baseline configurations on an annual basis, when required due to environmental changes, and during information system component installations and upgrades. (CM-2)

- Maintain a baseline configuration for information system development and test environments that is managed separately from the operational baseline configuration. (CM-2)

- Apply more restrictive security configurations for sensitive systems, specifically systems containing HIPAA data. (CM-2-COV)

- Modify individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning. (CM-2-COV)

The absence of baseline configurations increases the risk that these systems will not meet the minimum security requirements to protect data from malicious access attempts. Baseline security configurations are essential controls in information technology environments to ensure that systems have appropriate configurations and serve as a basis for implementing or changing existing information systems. If a data breach occurs to a system containing HIPAA data, the agency can incur large penalties, up to $1.5 million.

DBHDS should dedicate the necessary resources and prioritize the installation of the software to establish and maintain security baseline configurations for their sensitive information systems to meet the requirements in the Security Standard. Doing this will help ensure the confidentiality, integrity, and availability of the agency's sensitive data.

Improve Web Application Security
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Partial (first issued in fiscal year 2018)

DBHDS is not meeting some of the minimum requirements in the Security Standard for the web application. DBHDS uses the web application for wage employees, such as nurses and clinical staff, at the agency's 13 facilities. The web application is the originating system for wage employee hours and interfaces with the Commonwealth's payroll system. During fiscal year 2019, DBHDS had wage payroll totaling over $13.7 million making the integrity and availability of the web application critical to the agency. The following weaknesses exist for the web application:

- DBHDS only has one central administrator that manages and maintains the web application. Each facility has an administrator to handle small issues at their facility; however, the one central administrator at the Central Office is the only one responsible for tasks such as reviewing audit reports, setting up and configuring pay rules, granting and modifying administrator access for the facilities, and monitoring system performance. The Security Standard, Section AC-2-COV, requires DBHDS to have at least two individuals with administrator accounts to each IT system to provide continuity of operations. By having one administrator, DBHDS increases the risk of disruptions to the wage payroll process at the facilities in the absence of the single administrator.

- DBHDS did not update the risk assessment after the web application went through a recent upgrade to the software and web servers. The Security Standard, Section RA-3, requires DBHDS to update the risk assessment on an annual basis or whenever there are significant changes to the information system or environment. Without completing new risk assessments when a system undergoes a significant modification, DBHDS may not identify risks to the system and implement the necessary mitigating controls.

The primary contributing factor to these security weaknesses is the lack of resources dedicated to administer the web application. The IT security group is working on updating the risk assessment and expects to complete it in early fiscal year 2020.

DBHDS should hire or assign an individual to be a backup to the central administrator. DBHDS should update the risk assessment to ensure sufficient mitigating controls are in place. Doing this will help to ensure DBHDS maintains the confidentiality, integrity, and availability of their mission critical and sensitive systems.

Create Processes for Review and Assessment of Third-Party Service Provider's Controls
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

DBHDS does not have a formal process for identifying third-party service providers and evaluating their controls. DBHDS is not gaining annual assurance over the internal controls of two third-party service providers through review of Service Organization Control (SOC) reports or similar independent attestations. Specifically, for the third-party configuration of a system to support inpatient and long-term care functions for twelve DBHDS facilities, as well as, third-party administration of healthcare benefits for off-campus medical services provided to patients under DBHDS care. DBHDS relies on the provider of healthcare benefits to accurately calculate rates and discounts associated with charges from off-campus medical service providers. Additionally, both providers are responsible for the secure storage and transfer of patient data protected by HIPAA.

The Security Standard, Section SA-9-COV 3.1, requires agencies to perform an annual security audit of the environment or review the annual audit report of the environment conducted by an

independent, third-party audit firm on an annual basis. Furthermore, the contract terms for the inpatient and long-term care system state that DBHDS shall ensure performance of a Type 2 SOC audit at least once annually.

Without performing a review of SOC reports or similar attestations, DBHDS cannot ensure that third-party service provider's controls are designed, implemented, and operating effectively. This increases the Commonwealth's risk that it will not detect a weakness in a provider's environment, thereby exposing the Commonwealth to potential vulnerabilities created by third-party service providers. According to management, there is currently not a process in place for identifying and evaluating the controls of significant third-party service providers as they relate to finance. Additionally, management does not see the need to obtain assurance over the internal controls of the third-party service provider responsible for the administration of health care benefits for off-campus medical care.

DBHDS should create a documented process for identifying third-party service providers and assessing controls. DBHDS should consider which of its outsourced services merit a review of SOC reports or other attestations and should then document the results of its reviews in order to ensure the effectiveness of the third-party service providers' controls. If weaknesses are identified in the SOC reports or other attestations, DBHDS should implement complementary controls to mitigate the risk to the Commonwealth until the provider corrects the deficiency.

Why the APA Audits Compliance with Federal Requirements

DBHDS spends approximately $111 million in federal dollars annually, with over 77 percent of these funds being passed through to a subrecipient. Not complying with federal requirements for these funds could lead to the loss of federal funding. We reviewed compliance with federal requirements for the following programs: Substance Abuse Block Grant and the Opioid State Targeted Response (STR) and State Opioid Response (SOR) grants.

Implement Opioid Grant Subrecipient Monitoring

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

DBHDS is not properly monitoring the awards provided to Community Service Boards (CSBs) for the opioid grants as determined by DBHDS's Office of Budget and Financial Reporting's CSB Risk Assessment. DBHDS management responsible for the opioid grants did not have sufficient documentation of onsite visits with the CSBs to monitor programmatic progress for both the STR Grant and the SOR Grant that encompass the Catalogue of Federal Domestic Assistance (CFDA) 93.788.

The Code of Federal Regulations (CFR) 45 CFR § 75.352(6)(b) requires an evaluation of each subrecipient's risk of noncompliance with Federal statutes, regulations, and the terms and conditions of the subaward for purposes of determining the appropriate subrecipient monitoring described in paragraphs (d) and (e) of this section.

45 CFR § 75.352(6)(d) requires monitoring the activities of the subrecipient as necessary to ensure that the subaward is used for authorized purposes, in compliance with Federal statutes, regulations, and the terms and conditions of the subaward; and that subaward performance goals are achieved.

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

The SOR grant was new for the fiscal year, and DBHDS did not have a structured and coordinated internal process for the monitoring of the SOR Grant. Insufficient and unreasonable evidence of subrecipient monitoring activities could result in unallowable expenses and jeopardizes current and future funding. Current monitoring activities provide no authoritative proof that the CSBs are providing the services as outlined in the performance contract between DBHDS and the CSBs. The state, through DBHDS, is liable to the federal government for any funds that CSBs do not spend correctly.

DBHDS should properly document subrecipient monitoring over the opioid grants to ensure that CSBs are properly following federal requirements. Further, DBHDS management should improve communication effectiveness between DBHDS's subrecipient monitoring departments for compliance with the Code of Federal Regulations.

Provide Federal Award Requirements to Subrecipients
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

DBHDS is not providing federal award requirements to the CSBs for the opioid grants. DBHDS did not have a performance contract in place with the CSBs for the funding of the SOR Grant. A review of the CSB's performance contracts determined that the SOR Grant funding awarded to the CSBs from DBHDS did not exist. The SOR Grant accounts for $12,476,526 of $19,862,333 (62.81%) of total federal awards passed-through to the CSBs for opioid related services.

45 CFR § 75.352(a) requires every subaward be clearly identified to the subrecipient as a subaward and include certain information at the time of the subaward and if any of these data elements change, include the changes in subsequent subaward modification. When this information is not available, the pass-through entity must provide the best information available to describe the federal award and subaward.

The lack of a performance contract or memorandum of understanding outlining the requirements of the SOR Grant increases the risk of the CSBs using the awards for activities not related to the opioid grant or for unallowable costs associated with the opioid grant. This creates a potential

financial liability for DBHDS, and they have limited recourse with the CSBs due to the lack of a legally binding document.

The SOR Grant is a new grant, and DBHDS management assumed that the SOR Grant was covered in the existing performance contracts with the CSBs for fiscal year 2019. Therefore, DBHDS management did not have an addendum with the CSBs to cover the SOR Grant funding.

DBHDS should provide CSBs with the federal requirements attached to their federal awards. CSBs will be aware of the requirements of the federal awards, and DBHDS will be able to properly monitor whether the CSB complies federal regulations set forth in the contract.

Why the APA Audits Access to the Internal Accounting and Patient Revenue Systems

DBHDS utilizes internal systems for their accounting and financial reporting as well as patient revenue functions. Financial information in the internal systems impacts the financial information reported in the Commonwealth's accounting and financial reporting system. The Commonwealth's accounting and financial reporting system is the financial system that the Department of Accounts (Accounts) uses to report the Commonwealth's financial activity. Because these systems are critical to financial reporting to the Commonwealth, management at DBHDS must properly control access to ensure the integrity of data within these systems. To determine if system access was adequate, we reviewed access controls and compared DBHDS practices to those required by the Security Standard.

Improve Access Controls over the Internal Accounting and Patient Revenue Systems

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in 2018)
Prior Title: Improve Access Controls over the Internal Accounting System

DBHDS does not have written policies and procedures over access to their internal accounting and financial reporting system. The most recent policies and procedures are from 2006, which are outdated and do not reflect changes that were implemented during the system upgrades that occurred during 2011 and 2015. In addition, DBHDS does not have adequate policies and procedures over the granting and monitoring of access to the internal patient accounting system. DBHDS does not have a formal process in place to monitor access periodically to the internal accounting and financial reporting system. Specifically, we found the following issues with user access to internal systems:

- Three out of 25 (12%) users tested had access to the internal accounting and financial reporting system that did not agree with the access level on the user access form. Although DBHDS granted some levels of access to the employees upon request, account modification forms were created at the time of the auditor's request to reflect actual access in the system at the time of our inquiry.

- One out of two (50%) terminated users tested had access to the internal accounting and financial reporting system that was not removed within 24 hours. Removal for this user took four days after termination.

- Four out of 13 (31%) users tested had access in the internal patient revenue system but did not have an access form on file at the time of auditor inquiry. These users have had access to the system since prior to the implementation of access forms. Therefore, DBHDS performed the documentation of access forms for the users retroactively.

In addition, we found that monitoring requests over the internal accounting and financial reporting system for Central Office users were not sent out to department managers until after the end of the fiscal year. Furthermore, the Information Security Office did not ensure confirmation of proper access from each facility during the fiscal year as at least six facilities did not respond to monitoring requests until after the end of the fiscal year. We noted that monitoring requests do not include requirements as to timeliness of review, which would ensure that timely monitoring of access occurs.

The Security Standard, Section PS-4, states an organization must disable information system access within 24 hours of employee separation and terminate any authenticators or credentials associated with the individual. The Security Standard, Section AC-6, requires granting access based on the principle of least privilege and only authorizing user access, which is necessary to accomplish tasks in accordance with organizational missions and business functions. Part 7 of Section AC-6 requires the performance of an annual review of access to validate that the need of such access still exists.

Not ensuring that system users have and retain appropriate access to the internal accounting and financial reporting system increases the risk of unauthorized individuals inappropriately entering or approving transactions and could affect the integrity of DBHDS transactions in the internal and Commonwealth's accounting and financial reporting systems. Without a review of all accounts on an annual basis, DBHDS cannot verify that each user's access is appropriate based on job functions, does not violate the principles of least privilege or separation of duties, and is configured appropriately. Due to an increased workload and lack of staff resources, personnel did not update internal policies and procedures over the internal accounting and financial reporting system. Personnel in the Information Security Office did not understand the purpose and timing of when to perform monitoring activities, which should be done regularly during the fiscal year rather than only prior to the audit.

DBHDS should establish and implement proper policies, procedures, and controls over access to the internal accounting and financial reporting system, as well as the internal patient revenue system. DBHDS should ensure that monitoring of access to the internal accounting and financial reporting system for all facilities and the Central Office occurs annually and throughout the year as opposed to at the time of auditor's request.

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

All of the facilities within DBHDS do not have access management procedures, which meet the baseline standard defined by the Security Standard. The Information Security Office issued baseline procedures and implemented an application to approve access requests for all DBHDS facilities. However, the facilities have not developed procedures they can adapt for their specific environment that will ensure compliance with the Security Standard.

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

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

Promptly Remove Commonwealth's Accounting and Financial Reporting System User Access
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

DBHDS did not timely request that Accounts remove seven out of 20 (35%) Commonwealth's accounting and financial reporting system users access for individuals who no longer required access. Access removal requests for these users took between six to 64 days. Although DBHDS did have policies and procedures that included processes for removing access to the Commonwealth's accounting and financial reporting system, these procedures did not speak to the access removal timeframe.

The Security Standard, Section AC-2-COV 2f, requires the prompt removal of access when no longer needed. Per Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic 70220, security officers are responsible for submitting timely security deletion requests for staff who no longer require access. CAPP Manual Topic 70220 states that agencies should have policies and procedures that include processes for removing access timely for employees that have left the agency. Furthermore, DBHDS should ensure that these procedures are in compliance with the Security Standard.

Due to ineffective access controls, DBHDS did not ensure that individuals were removed timely from the Commonwealth's accounting and financial reporting system. Instead of promptly removing access upon termination, transfer, or layoff, security officers waited until the annual review of access to request the removal of employee's access. Delaying the removal of all access privileges increases the risk that former employees will have unauthorized access to Commonwealth systems and sensitive information.

Security officers should promptly remove access upon termination, transfer, or under other circumstances in accordance with the Security Standard. Security officers should submit timely security deletion requests to Accounts instead of waiting until annual access reviews to remove access. Additionally, DBHDS should strengthen internal policies and procedures over access to the Commonwealth's accounting and financial reporting system to ensure compliance with the Security Standard.

Why the APA Audits the Individual DBHDS Facilities

DBHDS is decentralized in nature and operates 13 facilities throughout the Commonwealth along with a Central Office. Since each facility has their own processes and procedures, we performed testwork over expenditure and journal entry transactions, financial system reconciliations, retirement benefits, and employment eligibility at the individual facilities and the Central Office. During the fiscal year, we tested the Central Office and the following facilities: Central Virginia Training Center, Eastern State Hospital, Southeastern Virginia Training Center, and Southwestern Virginia Mental Health Institute.

Improve Controls Over Financial Systems Reconciliations
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

Individual facilities within the DBHDS and the Central Office do not have adequate controls in place to ensure reconciliations between DBHDS and the Commonwealth's financial systems include a review of necessary reports, are performed timely and at the appropriate level, are materially correct, are signed by the preparer, and are properly reviewed. During our review, we found the following:

- Two of four facilities tested (50%) and the Central Office do not have adequate internal policies and procedures over the fixed assets reconciliation.

- One of four facilities tested (25%) did not have evidence of a proper reconciliation of appropriations and allotments.

- The Central Office did not have evidence of a proper reconciliation of capital appropriations and allotments.

- One of four facilities tested (25%) used the increase/decrease amount for an account rather than the proper month end balance on the fixed assets reconciliation.

- The Central Office does not review reports from the Commonwealth's fixed assets system during the reconciliation of fixed assets to ensure system totals agree.

- One of four facilities tested (25%) and the Central Office did not perform reconciliations at the appropriate level, specifically for expenses (fund, program, account level) and capital project expenditures (fund, project, and account level), respectively.

- One of four facilities tested (25%) and the Central Office did not have evidence of preparer signature and date for the monthly reconciliation, including the reconciliation of fixed assets.

- One of four facilities tested (25%) did not have evidence of a timely review by approver of the fixed assets reconciliation. In addition, the Central Office did not perform a proper review of a reconciliation.

CAPP Manual Topic 20905 prescribes the level of detail at which agency records, accounts, and logs must be reconciled depending on the nature of the transactions and requires documentation to be made available for inspection by outside parties. In addition, CAPP Manual Topic 30905 requires that the agency reconcile all agency source records to reports from the Commonwealth's fixed assets system. Finally, by submitting the Certification of Agency Reconciliations to Accounts, the agency is certifying that its internal records are in agreement with those reported in the state-wide financial system and that appropriations, allotments, expenses, capital project expenses, revenues, cash, fixed assets, and all other accounts have been reconciled at the appropriate level. This certification is required to be submitted by the last business day of the month following period close or as stated otherwise by the Comptroller.

The improper reconciliation of systems to the Commonwealth's accounting and financial reporting system increases the risk of material misstatement of overall account balances. These misstatements can ultimately affect funding for DBHDS services and the amounts DBHDS reports for the Commonwealth's Comprehensive Annual Financial Report (CAFR).

DBHDS facilities and the Central Office provided several reasons for the issues noted above. Facilities acknowledged that the exceptions occurred due to oversight error, unawareness of specific reconciliation requirements, and the fact that they did not retain documentation. We noted that the Central Office monthly reconciliations lack oversight and review by management. In addition, the Central Office's Budget Department maintains responsibilities over fixed assets. However, we found that the Fiscal Accounting Department lacks collaboration with the Budget Department during the fixed assets reconciliation.

Fiscal departments should reinforce policies and procedures over system reconciliations for DBHDS facilities and the Central Office. Management should communicate CAPP Manual requirements reflected in policies and procedures to personnel and ensure that the requirements are adhered to when

completing reconciliations. DBHDS should ensure that the appropriate preparer and reviewer sign each reconciliation and that a proper review is performed. Facilities and the Central Office should reconcile at the correct level and use proper ending balances for the monthly reconciliation. The Central Office Fiscal Accounting and Budget Departments should collaborate during the reconciliation of fixed assets. Finally, DBHDS facilities and the Central Office should submit monthly certifications to Accounts only after they complete all reconciliation requirements.

Process Expense Reimbursements in the Commonwealth's Accounting and Financial Reporting System

Type: Internal Control
Severity: Significant Deficiency
Repeat: No

One facility within DBHDS is not processing expense reimbursements in the Commonwealth's accounting and financial reporting system. Currently, the Fiscal Department (Fiscal) at the facility is processing expense reimbursements with a local petty cash account. Although the facility approves travel expenses prior to an employee's travel, the facility is not processing transactions as required in the Commonwealth's accounting and financial reporting system. As a result, the facility issued numerous travel advances to employees during the fiscal year using petty cash funds, amounting to $43,647.

CAPP Manual Topic 20335 requires state employees to be reimbursed for travel related expenses using the Travel and Expenses module of the Commonwealth's accounting and financial reporting system. Petty cash may not be used for travel advances to state employees. In addition, CAPP Manual Topic 20336 requires the processing of cash advances in the system. Processing of transactions in the Commonwealth's accounting and financial reporting system is important for ensuring transparency and proper accounting of transactions. The facility is at elevated level of risk for fraud, waste, abuse, and non-compliance if accounts are set up outside of the Commonwealth's accounting and financial reporting system. Finally, CAPP Manual Topic 20360 requires employees who travel overnight more than two times per year to be issued a travel charge card in order to reduce the need for travel cash advances.

Due to turnover at the facility, Fiscal staff did not maintain documentation of permission given by Accounts authorizing the use of a local account for reimbursements. Therefore, Fiscal staff were unable to provide documentation of approval to use the account for expense reimbursements. Additionally, staff were unaware of the CAPP Manual requirements for expense reimbursements and cash advances. Fiscal should process expense reimbursements in the Commonwealth's accounting and financial reporting system in accordance with applicable guidance. Fiscal management should ensure that staff understand the requirements associated with employee reimbursements and cash advances. Furthermore, employees that travel regularly during the year should be issued a travel charge card as required by the CAPP Manual.

Improve Controls over the Purchasing Process
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in 2018)

DBHDS is not ensuring compliance with the prompt pay provisions of the Virginia Public Procurement Act and is not properly processing purchase orders through the Commonwealth's purchasing system. The identified issues are as follows:

- Two of 16 (12.5%) expenses reviewed at one of the four facilities tested (25%) were not paid within the time requirements set by the prompt payment provisions.

- At one of the four facilities tested (25%), Fiscal did not ensure that the vendor charged the correct rate for services, which resulted in a payment at an incorrect amount.

- The Purchasing Department (Purchasing) did not properly process purchase orders through the Commonwealth's purchasing system for seven of 26 (26.9%) expenses reviewed at two of the four facilities tested (50%).

The untimely payments were due to a lack of communication between Fiscal and Purchasing. This resulted in one payment being included in the incorrect fiscal year, and overdue invoices ranging from 105 to 302 days. Code of Virginia § 2.2-4347 requires state agencies to pay for delivered goods and services within 30 days after receipt of a proper invoice or 30 days after receipt of the goods or services, whichever is later. By not following prompt pay requirements established by the Commonwealth, individual facilities may harm the Commonwealth's reputation as a buyer, damage relationships with vendors, and could incur late fees. Furthermore, Section 10.11 of the Agency Procurement and Surplus Property Manual (APSPM) encourages agencies with separate fiscal and purchasing departments to develop a Memorandum of Understanding to effectively resolve discrepancies and ensure timely payment.

Fiscal staff did not perform a proper review of the invoice and purchase order prior to approving the payment to ensure the vendor charged the correct rate, which resulted in a payment at the incorrect amount. CAPP Manual Topic 20315 states that the receiving report and purchase order should be obtained and matched to the corresponding invoice prior to approval and payment processing. Without properly matching the invoice to supporting documentation, the agency risks incorrect payment for goods or services.

Facility purchasing departments did not properly process purchase orders related to food service or pharmaceutical drug expenses. As a result, these payments were not supported by purchase orders from the Commonwealth's purchasing system. Facility purchasing departments were unaware of the requirement and noted processing pharmaceutical purchases through the Commonwealth's purchasing system would delay compliance with the vendor's payment terms. Section 14.9 of the APSPM requires the use of the Commonwealth's purchasing system for certain purchase transaction types. The APSPM

states that the purchase of pharmaceuticals is a transaction type that is exempt from agency and transaction fees imposed by the Commonwealth's purchasing system; however, use of the system is still mandatory. Without the mandatory use of the Commonwealth's purchasing system for certain purchases, there is an increased potential for reduced transaction transparency, analysis, and reporting.

DBHDS should ensure compliance with the prompt pay provisions through a clearly established process to resolve discrepancies between the Fiscal and Purchasing Departments timely. Fiscal should be trained to properly review invoices and purchase orders prior to approval and payment processing. Management at the individual facilities should improve purchasing processes and controls to ensure the proper use of the Commonwealth's purchasing system.

Perform an Evaluation and Analysis of Potential Asset Retirement and Pollution Remediation Obligations

Type: Internal Control
Severity: Significant Deficiency
Repeat: No

DBHDS did not perform a proper evaluation and analysis of potential asset retirement and pollution remediation obligations. Finance and Administration did not properly evaluate the applicability of Governmental Accounting Standards Board (GASB) Statement No. 83, *Certain Asset Retirement Obligations*, which became effective for reporting periods after June 15, 2018, and is applicable to fiscal year 2019. In addition, Finance and Administration did not perform any further consideration of GASB Statement No. 49, *Accounting and Financial Reporting for Pollution Remediation Obligations.*

Accounts performed a statewide survey for completion by all Commonwealth agencies to determine the applicability of this standard to the Commonwealth's financial statements. Based on the survey responses, all DBHDS facilities responded that they do not have any potential asset retirement obligations as defined by GASB Statement No. 83. We followed up on their responses and determined that DBHDS may have potential asset retirement obligations or pollution remediation obligations. We found, at a minimum, ten assets that should be further evaluated as a retirement obligation or remediation obligation. Further inquiry indicated that these identified assets did not meet the criteria of GASB 83.

Finance and Administration did not perform any verification of the individual facilities responses to the survey. Instead of performing their proper due diligence, Finance and Administration followed up with the Office of Architectural and Engineering at the Central Office as a reasonableness check of the facilities responses. Due to a lack of communication with the individual facilities, Finance and Administration was unaware of potential pollution remediation obligations and asset retirement obligations. Not contacting the facilities with direct knowledge of their assets risk incorrect responses to Account's survey. Further, not properly identifying potential asset retirement obligations or pollution retirement obligations could result in a misstatement of the Commonwealth's financial statements.

Finance and Administration should evaluate and analyze the impact applicable GASB standards have on the Commonwealth and DBHDS. This evaluation should take into consideration any applicable

external laws, regulations, contracts, or court judgements that DBHDS abides by that may trigger potential asset retirement obligations. Additionally, DBHDS should determine whether an obligating event has occurred that would cause recognition of pollution remediation obligations. Finance and Administration should coordinate with the proper personnel at the individual facilities to ensure adequate and accurate identification and accounting of potential asset retirement obligations and pollution remediation obligations.

Why the APA Audits Compliance with Employment Eligibility Guidelines

DBHDS employs over 6,000 employees, hiring a significant number each year. Noncompliance with federal government employment eligibility guidelines could result in financial penalties. To determine compliance with the employment eligibility process, we reviewed the individual facilities processes and forms used to verify both employment eligibility and identity. We compared their processes to those required by the federal government and the Code of Virginia.

Comply with Employment Eligibility Requirements

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

Individual facilities within the DBHDS do not have sufficient processes and controls over the employment eligibility process. Employment Eligibility Verification forms (Form I-9) are not completed by the Human Resources Departments (Human Resources) at the facilities in accordance with guidelines issued by the United States Citizenship and Immigration Services of the Department of Homeland Security. During fiscal year 2019, we noted the following:

- Human Resources could not locate Form I-9 for one out of 40 (2.5%) employees tested.
- Human Resources did not fully complete Section 2 of the Form I-9 for 11 out of 40 (27.5%) employees tested.
- Human Resources did not ensure that the employee properly completed Section 1 of Form I-9 for one out of 40 (2.5%) employees tested.
- Human Resources at three out of four (75%) facilities tested and the Central Office did not have written policies and procedures over employment eligibility.

The Immigration Reform and Control Act of 1986 requires that all employees hired after November 6, 1986, have a Form I-9 completed to verify both employment eligibility and identity. The United States Citizenship and Immigration Services sets forth federal requirements for completing the Form I-9 in the Handbook for Employers known as the M-274. Per M-274, the employer is responsible for ensuring all parts of Form I-9 are completed and retained for a period of at least three years from the

date of hire or for one year after the employee has separated, whichever is longer. Not complying with federal requirements could result in civil and/or criminal penalties and debarment from government contracts.

The issues listed above occurred because Human Resource staff at the facilities have not received proper training in this area. Further, Human Resources is not performing an adequate review of Form I-9's to ensure the proper completion of the form. Management should provide adequate training to Human Resources staff to reinforce the expectation of compliance with the applicable federal requirements. Human Resources should perform an adequate review of Form I-9's completed by staff and employees to ensure accurate completion and compliance with federal requirements. Additionally, Human Resources should develop and implement policies and procedures over employment eligibility.

Why the APA Audits Payroll

DBHDS employs over 6,000 salaried and wage employees across the 13 facilities and Central Office. DBHDS' payroll expenses exceeded $405 million during the fiscal year. Because of the sizeable nature of this expense to the Commonwealth, DBHDS management must take necessary precautions to ensure the integrity of payments to employees. To determine whether DBHDS' payroll controls were adequate, we compared agency practices against their own policies as well as the requirements set by Accounts and Department of Human Resource Management (Human Resource Management). During the fiscal year, we tested various payroll controls at all DBHDS facilities and the Central Office.

Perform Reconciliation between the Commonwealth's Payroll and the Accounting and Financial Reporting Systems

Type: Internal Control
Severity: Significant Deficiency
Repeat: No

DBHDS is not reconciling the Commonwealth's payroll system to the Commonwealth's accounting and financial reporting systems as part of their post-certification process for payroll. All four of the DBHDS facilities reviewed (100%) and the Central Office did not perform a reconciliation between the two systems during payroll post-certification activities.

Facility and Central Office payroll departments perform a monthly reconciliation of the Commonwealth's accounting and financial system and the agency's internal accounting system. The reconciliation shows overall payroll expenses between the systems; however, it does not go into the necessary detail. CAPP Manual Topic 50820 requires a review of payroll expenses recorded in the Commonwealth's accounting and financial reporting system to ensure that all expenses were recorded correctly. The topic outlines reports that should be included in the review process, which includes reports from both the payroll and accounting and financial reporting systems. An adequate and complete post-certification process ensures payroll expenditure data is accurate and complete. Without reconciling the two systems, DBHDS is unable to ensure that they are charging payroll expenses to the

correct programmatic codes. Furthermore, not performing the reconciliation may cause errors or discrepancies in either system to go undetected.

Facilities and the Central Office should implement a process to reconcile the Commonwealth's payroll and the Commonwealth's accounting and financial reporting systems as part of their post-certification process for payroll in accordance with the CAPP Manual.

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

DBHDS needs to improve controls over payroll certifications. We found that all four facilities tested and the Central Office do not have adequate controls over the payroll certification process. Specifically, we found the following:

- Two facilities and the Central Office (60%) do not have adequate, written policies and procedures over the payroll certification process that are in line with the CAPP Manual.

- One of the four facilities reviewed (25%) is not following internal payroll certification policies and procedures for wage certifications.

- Three of the four facilities (60%) tested did not review all necessary reports during the payroll pre- and post-certification process.

- Two of the four facilities (50%) reviewed do not have an adequate process in place to perform a regular comparison between the Commonwealth's payroll and human resources systems during post-certification.

- One of the four facilities (20%) reviewed does not have proper separation of duties within the facility's payroll function.

CAPP Manual Topic 20905 requires that agencies have written policies and procedures separate from the CAPP Manual for all processes. CAPP Manual Topics 50810, 50815, and 50820 outline procedures over the certification process, including pre- and post-certification requirements. CAPP Topics 50810 and 50820 require the review of specified reports from the Commonwealth's payroll system during payroll pre- and post-certification review respectively. In addition, as a best practice, there should be a separation of duties between all critical parts of the certification process.

DBHDS staff were unaware that procedures should exist separate from the CAPP Manual. The lack of formally documented internal policies and procedures that are customized to reflect the agency's staffing, organization, and unique operating procedures exposes the agency to unnecessary risk of performing payroll certifications improperly. In addition, written procedures reduce the impact that turnover has on institutional knowledge. The Central Office has not reviewed the Payroll Service Bureau

Scope of Services manual since it was last updated in 2016. Without a regular review of this manual, the Central Office may neglect to fulfill responsibilities as outlined by the Payroll Service Bureau.

Many of these exceptions occurred because the individual facilities and the Central Office do not have adequate policies and procedures over the payroll process. In addition, we found in most cases that payroll staff do not review or maintain documentation of reports if no exceptions are found during the certification review.

Facility and Central Office payroll departments should improve existing policies and procedures over the payroll certification process or develop procedures if they do not already exist. Facility and Central Office payroll departments should ensure that applicable staff review all necessary reports throughout the payroll certification process and ensure that these reports are retained as part of the certification file.

Develop Access Profile Descriptions and Improve Monitoring Controls over the Internal Attendance and Leave System

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

DBHDS does not have descriptions of access profile capabilities for the internal time, attendance, and leave system. Since each DBHDS facility has the option to request access profiles based on the facility's need, there are varying profiles across all facilities and the Central Office. Additionally, documentation of access monitoring was not in compliance with internal monitoring requirements, which requires a complete review of all user access to be performed annually. We completed a review of monitoring certifications and submissions for all 14 DBHDS facilities and the Central Office. Four facilities (27%) did not include evidence that all access types were reviewed for reasonableness on their monitoring spreadsheets. Two of these facilities only documented the monitoring of users with elevated access privileges and users with unreasonable access that required a change. The other two facilities only documented unreasonable access.

The Security Standard, Section 8.1 AC-1, requires agencies to develop, document, disseminate, and review and update annually, an access control policy that addresses purpose, scope, roles, compliance, and responsibilities and formal documented procedures to facilitate the implementation of the policy and associated access controls. Additionally, Section 8.1 AC-2 of the Security Standard states "the organization reviews accounts for compliance with account management requirements on an annual basis or more frequently if required to address an environmental change."

Access descriptions are important to properly assign profiles to new users and help to ensure least privilege. Written documentation reduces the impact that turnover has on institutional knowledge and makes information more readily available. The lack of proper monitoring of all users can result in inappropriate access such as access for terminated employees. In addition, inadequate system documentation may cause inefficiencies in the process of granting access as well as monitoring of access.

DBHDS has not developed access profile descriptions due to the lack of staff and resources. Inadequate documentation of access monitoring occurred due to the new monitoring process implemented during fiscal year 2019 which requires the review of all users as opposed to only those with elevated access privileges. The facilities that did not comply with the new internal monitoring requirements were still following the historical monitoring process.

DBHDS should develop access capability descriptions for access profiles for the internal time, attendance, and leave system. In addition, all DBHDS facilities and the Central Office should perform and document a complete review of all users at least annually. The Central Office should review all facility submissions to ensure completeness of access reviews.

Improve Review Process for Individual Facility Leave Liability Submissions
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

DBHDS needs to strengthen its controls over the review and reporting of the year-end agency leave liability submission to Accounts. The Office of Budget Execution and Financial Reporting (Budget Execution) at the Central Office receives and compiles individual facility leave liability submissions, which include leave liability and the detailed calculations behind it. Budget Execution performs a compilation of this support in order to report the total leave liability for DBHDS on the Leave Liability Attachment to Accounts for inclusion in the Commonwealth's financial statements. Budget Execution does not perform an adequate review of these submissions to ensure that the total current and noncurrent leave liability reported is accurate. In addition, each of the four facilities reviewed in detail has their own unique process of calculating and reviewing leave liability. The following errors were noted on the leave liability submission, the supporting documentation, and facility review processes:

- Budget Execution reported $2,357,321 of leave liability in the incorrect fund on the Leave Liability Attachment.

- Budget Execution reported $38,202 of leave liability in the incorrect program in support used for preparation of the Leave Liability Attachment.

- One facility did not use the correct social security base to determine taxes on leave liability.

- One facility reported $800,877 of leave liability in the incorrect program on the facility's leave liability submission to Budget Execution.

- One facility performed an inadequate review of leave liability prior to submitting information to Budget Execution and does not have a formal review process in place at the facility.

The Comptroller's Directive No. 1-19 establishes compliance guidelines and addresses financial reporting requirements for state agencies to provide information to Accounts for the preparation of the CAFR as required by the Code of Virginia. The Comptroller's Directive also states that by submitting the

attachment to Accounts, the agency is certifying that the attachment has been reviewed and is accurate. This guidance also provides assistance to those who prepare and review financial reporting attachments and supplemental information sent to Accounts for presentation in the CAFR.

These errors occurred for multiple reasons. Budget Execution reported amounts in the incorrect fund on the Leave Liability Attachment due to human error not detected by the review process. Individual facilities are under the impression that Budget Execution performs a detailed review of facility leave liability submissions. However, Budget Execution assumes that an adequate review is performed at the facility level. Furthermore, due to turnover, one facility does not have a formal process in place for reviewing leave liability for accuracy once calculated by the preparer. Without an adequate review process, there is a higher risk of misstatement of current and noncurrent leave liability reported as part of the CAFR. This risk is elevated due to the fact that there is potential for inadequate reviews to occur at both the facility and Budget Execution level.

Budget Execution certifies the leave liability submission and; therefore, should enhance its review of individual facility submissions for accuracy prior to preparing its Leave Liability Attachment submission. Budget Execution should communicate with facility staff responsible for preparing the individual facility leave liability submissions throughout the financial reporting process to ensure all staff are aware of the correct reporting process, use the proper criteria for leave reports, and include all necessary leave balances for the calculation of leave liability.

Retain Documentation of Property Collection and Removal of Terminated Employee Badge Access
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

Individual facilities within the DBHDS do not have sufficient processes and controls over terminated employees. Two out of four (50%) facilities tested did not have formal termination processes. It should be noted that one of these facilities experienced a significant number of layoffs during the fiscal year. As a result, Human Resources at the facilities were unable to provide documentation confirming the collection of Commonwealth property or timely removal of badge access for all 24 of the terminated employees sampled at those facilities. Further, three facilities do not have internal policies and procedures over the employee termination process, although, one facility uses a termination checklist during the termination process.

CAPP Manual Topic 50320 recommends agencies develop a termination check-off list to complete as part of the termination process, to include the collection of outstanding uniforms, badges, keys, etc. Per CAPP Manual Topic 20905, agencies should develop internal policies and procedures aside from the CAPP Manual over all critical areas. DBHDS experienced significant turnover during the period under review, as evidenced by the fact that DBHDS employs over 6,000 employees and had over 1,700 separations during this period. Without proper and sufficient internal controls over terminated employees that ensure the return of Commonwealth property and removal of all access privileges, individual facilities are increasing the risk that terminated employees may retain physical access to

Commonwealth property and unauthorized access to state systems and sensitive information. For DBHDS, the exposure to risk is further increased due to the secure nature of the individual facilities.

These issues occurred because the individual facilities have not developed and implemented policies and procedures over the termination process. Individual facilities stated that they place reliance on the Human Resource Management termination procedures. Alternatively, facilities are unaware that separate written procedures are required. One facility used a termination checklist in the past, but is no longer using it during terminations. Further, facilities rely on verbal communications with employees to collect property. In addition, the Security Department is responsible for removing badge access; however, they do not retain evidence of the badge deactivation.

Management across all DBHDS facilities, not just those reviewed, should ensure that adequate processes and controls are in place over terminated employees. Individual facilities should develop and implement more effective termination processes to ensure the collection of Commonwealth property and the timely removal of badge access for terminated employees. Additionally, facility staff should retain documentation of terminations. Facilities should develop policies and procedures over the termination process and/or create a termination checklist if they do not already exist.

Ensure Terminated Employees Are Properly Classified in the Payroll System
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

Individual facilities within the DBHDS did not change the employment status for six terminated or inactive employees in the Commonwealth's payroll system. Four out of six (67%) terminated or inactive employees did not receive any compensation during the 2018 calendar year but remained "active" in the system after January 2019. Two out of ten (20%) employees identified that received their final paychecks remained "active" in the Commonwealth's payroll system after being terminated.

CAPP Manual Topic 50320 states that agencies must verify that information in the Commonwealth's payroll system concerning terminated employees is complete, properly authorized, and entered accurately into the system. Employees remaining active in the payroll system after being terminated and having received final paychecks pose a risk for improper payments.

The facilities did not properly identify and update the statuses of these employees due to a lack of management oversight. In addition, facility staff reactivated several employees in the Commonwealth's payroll system during the fiscal year in order to update their Federal Insurance Contributions Act statuses; however, staff did not change these employees back to an "inactive" status once changes were made. The facility recognized that more instances of this potentially exist and have since begun to correct this misclassification.

Facilities should ensure terminated or inactive employees are properly classified in the Commonwealth's payroll system. Facilities should regularly complete a review of employment statuses

to ensure employees terminated in the human resources system are removed from the Commonwealth's payroll system after final pay is made to the employee.

Improve Access Controls over the Commonwealth's Payroll System
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Individual facilities within the DBHDS and the Central Office are not consistently removing system access to the Commonwealth's payroll system for terminated or transferred employees in a timely manner. For three out of eight (38%) Commonwealth's payroll system users tested, payroll security officers at the individual facilities and the Central Office did not terminate employee access up until two to 76 days after their last day worked.

The Security Standard, Section PS-4, states an organization must disable information system access within 24 hours of employee separation and terminate any authenticators or credentials associated with the individual. Untimely termination of access from the Commonwealth's payroll system greatly increases the risk of unauthorized payroll transactions.

There are two underlying causes for why access to the Commonwealth's payroll system was not timely removed. Payroll security officers at the individual facilities and the Central Office thought that it was reasonable to remove access within two days and; therefore, they did not comply with the access removal timeframe stipulated in the Security Standard. Additionally, access was not promptly removed upon layoff because a payroll security officer waited until the semi-annual review of access to request the removal of employee's access.

Payroll security officers at the individual facilities and the Central Office should ensure that access to the Commonwealth's payroll system is promptly removed upon termination, transfer, or under other circumstances in accordance with the Security Standard. Further, staff should submit timely requests to delete access, instead of waiting until semi-annual access reviews to remove access. Payroll security officers should ensure compliance with access removal timeframes as outlined in the Security Standard.

Properly Approve and Monitor Administrative Employee Overtime
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

DBHDS should improve controls over employee overtime. During our review, we found that employees in administrative positions at two DBHDS facilities worked an excessive amount of overtime during the fiscal year that was not properly approved or was not reasonable in relation to job responsibilities. Specifically, two out of 18 (11%) employees tested worked overtime hours that was not properly approved, and one out of 18 (6%) employees tested worked overtime that is unreasonable in relation to the employee's responsibilities.

One of the facilities had a large increase in employee turnover during the fiscal year, and the lack of staff required existing staff to take on additional workload and overtime. Management at the second facility approved an administrative employee to work overtime because there was a misunderstanding of the employee's job roles and responsibilities. The Human Resource Management Policy 1.25, Hours of Work, states that non-exempt employees must not work additional hours that have not been authorized by management.

DBHDS facilities should improve controls over employee overtime by properly approving and monitoring administrative employee overtime hours. DBHDS should develop processes for monitoring and tracking hours for wage employees in administrative positions. Payroll departments should clarify with managers that overtime must be properly approved and reasonable in relation to employee job responsibilities. When possible, DBHDS should allocate additional staff as needed to mitigate excessive overtime hours on existing staff.

Why the APA Audits an Agency's Controls Over their Information in the Commonwealth's Retirement Benefits System

The Commonwealth's retirement benefits system is used to calculate the total pension liabilities for the Commonwealth. Individual agencies are responsible for updating the records within the retirement benefits system related to their employees. As a result, DBHDS management must take adequate precautions to ensure the integrity of these records. To determine if management implemented these precautions, we compared the individual facilities practices to the guidance provided by Accounts and the Virginia Retirement System (VRS).

Perform and Document Commonwealth's Retirement Benefits System Reconciliations

Type: Internal Control
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2014)
Prior Title: Improve Controls over the Commonwealth's Retirement Benefits System

Individual facilities within the DBHDS and the Central Office did not adequately perform and document reconciliations between the Commonwealth's human resource and retirement benefits systems during fiscal year 2019. Specifically, we noted the following:

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

- Three of the four facilities tested (75%) did not maintain documentation to support correction of all non-creditable compensation data discrepancies prior to confirming the contribution.

- One of four facilities tested (25%) did not clear exceptions identified on the Commonwealth's human resource system cancelled records reports in a timely manner.

- The Central Office and three of the four facilities tested (75%) are not confirming the contribution snapshot within the required timeframe.

- The Central Office and three of the four facilities (75%) tested only reviewed the cancelled record report monthly and could not provide adequate justification for their deviation from the CAPP Manual guidance.

CAPP Manual Topic 50410 requires a daily review of the human resource system cancelled record report. Reviewing and correcting items in the cancelled record report ensures retirement benefits are accurately calculated and properly transmitted between the human resource and benefits systems.

Additionally, CAPP Manual Topic 50410 states that agencies should perform a reconciliation of creditable compensation between the Commonwealth's human resource and retirement benefits systems monthly before confirming the contribution. Improper reconciliation processes can affect the integrity of the information in the Commonwealth's retirement benefits system that determines pension liability calculations for the entire Commonwealth. Since the VRS actuary uses retirement benefits system data to calculate the Commonwealth's pension liabilities, inaccurate data could result in a misstatement in the Commonwealth's financial statements.

In accordance with the Contribution Confirmation and Payment Scheduling VRS Employer Manual, all employers are required to submit the contribution snapshot for the month by the 10th of the following month. Not reviewing or reconciling the contribution snapshot prior to confirmation deadline can result in incorrect payroll deductions and retroactive collections.

Individual facilities staff were unsure of how to perform several components of the reconciliation process; therefore, they did not properly perform pieces of the reconciliation process during the fiscal year. Due to turnover, staff did not retain sufficient documentation that the reconciliation to the Commonwealth's retirement benefits system occurred. Additionally, due to the lack of understanding of documentation requirements, staff did not maintain documentation showing the clearing of all exceptions. Human Resources at the Central Office was unaware of the requirement to reconcile the human resources and benefits systems prior to confirming the monthly contribution. In addition, current written procedures do not include the reconciliation of the human resources and benefits systems. Human Resources staff at the Central Office are in the process of updating procedures over the reconciliation to be distributed agency wide.

Management should ensure that staff perform and document monthly reconciliations between the Commonwealth's human resource and retirement benefits systems. Staff should clear exceptions noted in the Commonwealth's human resource system cancelled record report timely. When clearing exceptions, staff should document the reason for the exception and the remediation activities performed. Management should implement corrective action to ensure that the contribution snapshot

is confirmed by the 10th of the following month. Additionally, management at the Central Office should ensure that policies and procedures include all necessary requirements for performing a reconciliation of the Commonwealth's human resources and benefits systems. Policies should include sufficient justification for any deviation from CAPP Manual requirements.

Improve Controls over Access to the Commonwealth's Retirement Benefits System
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in 2014)
Prior Title: Improve Controls over the Commonwealth's Retirement Benefits System

Individual facilities within the DBHDS and the Central Office do not have adequate controls in place to ensure that system access to the Commonwealth's retirement benefits system is appropriate. Human Resources at the facilities and the Central Office did not terminate system access timely to the Commonwealth's retirement benefits system for six out of 11 (54%) inactive users. Access removal for these users ranged between three days to 72 days post separation. One out of three active Commonwealth's retirement benefits system users tested (33%) at the Central Office had system access privileges that were neither appropriate nor based on least privilege according to job responsibilities.

The Security Standard, Section PS-4, states an organization must disable information system access within 24 hours of employee separation and terminate any authenticators or credentials associated with the individual. Delays in deleting access increases the risk of unauthorized use of the Commonwealth's retirement benefits system which could result in unauthorized changes and could impair data integrity.

Furthermore, Security Standard, Section AC-6, requires granting access based on the principle of least privilege and only authorizing user access which is necessary to accomplish tasks in accordance with organizational missions and business functions. Granting access based on the principle of least privilege is a best practice for maintaining security over critical systems. When access granted violates the principle of least privilege, there is an increased risk that users can circumvent other compensating controls and perform unauthorized transactions.

According to management at the individual facilities and the Central Office, timely removal of user access to the Commonwealth's retirement benefits system did not occur due to delayed communication within Human Resources. Further, Human Resources did not have a documented procedure for removing terminated employee access to the Commonwealth's retirement benefits system. For the user that had inappropriate access at the Central Office, Human Resources did not appropriately consider the principle of least privilege when establishing access.

Human Resources Management should ensure that access to the Commonwealth's retirement benefit system is appropriate. Human Resources at the individual facilities and the Central Office should ensure there are proper procedures in place to remove unneeded access to the Commonwealth's retirement benefits system timely. Human Resources at the Central Office should reassign access to the Commonwealth's retirement benefits system based on a least privilege basis as defined in the Security Standard.

Why the APA Audits Information System Security

The Department of Health (Health) collects, manages, and stores significant volumes of personal and financial data within its mission critical systems. Because of the highly sensitive and critical nature of this data, Health's management must take all necessary precautions to ensure the integrity and security of the data in its systems. We compared Health's practices to those required by the Security Standard in the areas of web application security, oversight of sensitive systems, and information systems access.

Improve Web Application Security

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

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

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

Health should implement the controls discussed in the communications marked FOIAE in accordance with the Security Standard and best practices in a timely manner.

Improve Contingency Management Program

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

Health does not perform certain processes in their contingency management program required by the Security Standard and industry best practices. We identified two weaknesses and communicated them to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to the descriptions of security mechanisms contained within the document.

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

Health should implement the controls discussed in the communication marked FOIAE in accordance with the Security Standard and best practices in a timely manner.

Improve the Disaster Recovery Plan
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Health does not perform certain processes in its disaster recovery plan required by the Security Standard and industry best practices. We identified a weakness in this area and communicated this to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to descriptions of security mechanisms contained within the document.

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

Health should implement the controls discussed in the communication marked FOIAE in accordance with the Security Standard and best practices in a timely manner.

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

Department supervisors did not notify the Office of Human Resources (Human Resources) in a timely manner as they became aware of employee separations, which resulted in delays of system access removal. Additionally, in some cases, the supervisors and Human Resources did not realize that the terminated employees had active accounts to certain information systems, causing delays in deleting the accounts. During our review, we found delays in the removal of access from the following information systems:

- Health removed access to the Commonwealth's human resources system for 105 users during the fiscal year, but did not remove access timely for three of these users. These accounts were removed 16 to 211 days after the employees' separation dates.

- Health removed access to the Commonwealth's payroll system for 37 users during the fiscal year, but access was not removed timely for four users. These accounts were removed 13 to 166 days after the employees' separation dates.

- Health removed access to the patient management system for 376 users during the fiscal year, but access was not removed timely for 24 users. These accounts were removed seven to 144 days after the employees' separation dates.

- Health removed access to the Commonwealth's accounting and financial reporting system for 32 users during the fiscal year, but access was not removed timely for one user. This account was removed four business days after the employee's separation date.

Section PS-4 of the Security Standard requires agencies to "disable information system access within 24 hours of employment termination." Additionally, Health's internal off-boarding procedure requires supervisors to inform Human Resources of an employee separation as soon as the supervisor is aware of the separation. Health's procedure then requires deletion of the account within 24 hours of notification.

Terminated employees who still have access to critical systems may be able to access these systems after leaving the agency. By not deleting users' accounts to sensitive information systems timely, this also increases the risk of an internal or external party compromising these unneeded accounts and using them to access these systems. Each of these scenarios increases the risk of inappropriate transactions and the exposure of sensitive data.

Health implemented a new process to off-board employees during the fiscal year to increase efficiency; however, there were still delays in removing system access in both the old and new processes. In some cases, department supervisors and district Human Resources staff did not complete their parts of the off-boarding process in a timely manner. In other cases, Health did not identify the fact that the terminated employees had access to these systems in order to remove the access. Additionally, Health's off-boarding process does not include a review of the off-boarding procedures to ensure each responsible party completed their tasks. Therefore, Health was not able to identify the fact that they needed to remove these users' access in a timely manner.

Health should strengthen their new process by implementing a review of all off-boarding tasks and clarify the timeline for each task. This will ensure completion of each task and will identify instances of delay. Health should also review system access listings with each employee termination to identify the systems the employees can access. This will reduce rates of non-compliance with both the statewide and internal policies by removing the access within 24 hours. This will also reduce the risk of unauthorized transactions and exposure of sensitive data. Health may also want to review their current policy to ensure it is in compliance with the Security Standard. Any policy exceptions to the Security Standard need to be approved by VITA.

Perform System Access Reviews
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Partial (first issued in fiscal year 2018)

Health did not perform comprehensive system access reviews within timeframes established by internal and statewide procedures. Health has multiple critical systems throughout several different departments. These systems support various business functions, including accounting, patient management and benefits administration, so there are various internal policies that address periodic system access reviews. During our review of Health's system access reviews, we identified the following instances of non-compliance with policies and procedures:

- Department supervisors did not submit three out of ten (30%) monthly access review certifications by the due date for the internal financial and accounting system; receipt of these certifications occurred 24 to 66 days past the due dates.

- Department supervisors did not submit three out of ten (30%) monthly access review certifications by the due date for the patient management system; receipt of these certifications occurred between seven to 16 days past the due dates.

- Human Resources has not performed a comprehensive annual review of access privileges for the Commonwealth's retirement benefits system since April of 2017.

- After implementing monthly access reviews for the Women, Infants, and Children (WIC) eligibility system in April 2019, 12 of 35 department supervisors did not submit at least one of their monthly access review certifications over the three-month period between April and June 2019. Two of these supervisors did not submit the certification for any of the three months. In addition, central office staff did not maintain any certifications or other evidence of a comprehensive access review for the same system throughout the entire fiscal year.

- Administrative staff did not perform two quarterly access reviews for the HIV formula grant system as required by Health's internal access review policy.

- Health has no formal process in place for reviewing access to the WIC electronic benefit system. Although a third party manages this system, Health employees have read-only access to information in the system but do not have a process to manage this access.

Health's internal policies require supervisors of Health's various business areas to review and certify access to Health's accounting, patient management, and WIC benefits systems monthly. For the patient management and accounting systems, the policy requires these supervisors to perform these monthly reviews by the tenth day of the following month. Health's internal policy on reviewing access to the HIV formula grant benefits system requires a quarterly review. Additionally, for sensitive

information systems, Section AC-6-7a of the Security Standard requires agencies to "review on an annual basis the privileges assigned to all users to validate the need for such privileges."

Regular access reviews ensure that system administrators processed all requests to add, modify or delete users properly and in accordance with requests from the system owners. Not performing regular access reviews increases the risk of individuals having inappropriate access to information systems

Staffing changes caused some of the delays in performing and certifying access reviews of the patient management and accounting systems. In some situations, the reviewer did not get the correct level of access to both review and certify system access in time to meet the deadlines. Resource constraints and the prioritization of other tasks led to the remaining delays in the patient management and accounting systems reviews as well as the retirement benefits system and WIC eligibility system reviews. Staffing changes were also the cause for the lack of reviews for the HIV formula grant benefits system.

Health should ensure backup personnel are available to perform regular reviews of access in the event that the primary reviewer is unable to perform the review. Additionally, Health should perform follow-up procedures when reviewers do not provide certifications within their established timeframes to ensure the prioritization of these reviews. This will reduce the rates of untimely reviews and decrease the risk of inappropriate access to sensitive information systems.

Why the APA Audits Human Resources and Payroll Processes

Health employs over 3,600 salary and wage employees throughout the state. Health's payroll and payroll-related expenses totaled over $263.5 million in fiscal year 2019, with $74.2 million (28%) being paid with federal funds. Additionally, Health's payroll and payroll-related expenses are significant and material to the statewide expenses reported in the state's CAFR. Employee information set up in the human resources and benefits systems drives many of Health's payroll and payroll-related expenses. Therefore, it is critical for Health to maintain adequate internal controls over both the Human Resources and Payroll processes. In order to evaluate these functions, we compared Health's processes to requirements outlined in statewide human resources and payroll procedures.

Perform Monthly Reconciliations of the Payroll and Retirement Systems

Type: Internal Control
Severity: Significant Deficiency
Repeat: No

Health has not performed monthly reconciliation procedures for the retirement benefits system since October of 2018. There are five automated reports, which show reconciling items between the payroll system and the retirement benefits system. These monthly reports ensure Health withholds the correct amounts from employees' paychecks and remits the correct amounts to VRS.

According to CAPP Manual Topic 50410, "exception items on automated VRS reconciliation reports should be identified and communicated to the proper system of authority for correction as soon as possible, but no later than 31 days from the date of the report." This same section of the CAPP Manual also requires agencies to "ensure that a timely review of the monthly reconciliation reports is performed and that any automated transfers are accurate or correcting actions are completed." Additionally, the Contribution Confirmation Section of the VRS Employer Manual states "…the employer should review and reconcile amounts in the retirement benefits system to the information in the payroll system." The lack of a reconciliation between the payroll system and the retirement benefits system also represents a violation of Health's internal policies and procedures.

Without performing reviews of monthly reconciliation reports, Health does not know if there are discrepancies between the payroll system and the retirement benefits system to report. The lack of a monthly review prevents Health from being able to identify and resolve reconciling items between the payroll system and the retirement benefits system. This could cause an improper deduction from an employee's paycheck or an incorrect remittance to VRS on an employee's behalf. Additionally, since the VRS actuary uses the retirement benefits system data to calculate the Commonwealth's pension liabilities, inaccurate data due to unresolved exceptions could result in a misstatement in the Commonwealth's financial statements.

Employee turnover in the Payroll Department caused Health to stop performing monthly reviews of the reconciliations due to the prioritization of other critical payroll tasks. Health recently hired an additional employee for the Payroll Department and provided training on these reconciliations. Health should continue to resolve the backlog of reviews and report any reconciling items for resolution. In addition, Health should provide cross-training and designate a backup person to perform this task in the future to prevent gaps in performance in the event of future turnover.

Strengthen the Employee Off-Boarding Process

Type: Internal Control
Severity: Significant Deficiency
Repeat: No

Health did not correctly complete their off-boarding procedures for employees who separated from the agency. Health underpaid an employee for their annual leave payout and did not detect this error. In addition, Health discontinued paying two employees who terminated their employment, but did not remove them from the Commonwealth's payroll system for an entire year following their separations.

As a result of an error in the leave payout calculation, Health underpaid an employee $2,067 in the employee's final paycheck and had to issue a corrected check. Additionally, not reporting employees as terminated in the payroll system led to the two employees remaining in the system throughout the fiscal year. Although Health discontinued paying these employees, leaving them in the payroll system increases the risk of accidentally paying the employees after termination. CAPP Manual Topic 50320 states that agencies must verify that the Commonwealth's payroll system information concerning terminating employees is complete, properly authorized, and entered accurately into the system.

Health does not have a review process in place to ensure the Payroll Department correctly completes each of its required off-boarding tasks. Additionally, each of these issues came at a time when Health experienced turnover and a high volume of transactions in the department. Resource strain and the lack of a review process contributed to Health reporting inaccurate and incomplete information to the payroll system.

Health should implement a review process of employee off-boarding documents to ensure all amounts keyed agree to the approved supporting documentation. This review process should also cover each step of the employee off-boarding process to ensure payroll analysts enter all terminations completely and accurately into the payroll system. This will reduce the risk of incorrectly paying terminated employees.

Enhance the Overtime Reporting Process

Type: Internal Control
Severity: Significant Deficiency
Repeat: No

Health paid one of its employees an incorrect amount of overtime pay and did not pay the overtime until over a month after the employee worked the overtime hours. This resulted in an overpayment of $4,889, which was not detected until the employee reported this issue to management.

CAPP Manual Topic 50505 requires agencies to properly complete and authorize all source documents used to pay employees. This ensures accurate entry into the payroll system. When a classified employee works overtime, Health requires managers to complete a "Classified Employee Overtime Form" (overtime form). This form requires the total number and type of overtime hours worked. The signing of this form serves as the certification that the employee worked the number of hours listed on the form.

As a result of the incorrect completion of this form, Health paid an employee an incorrect amount of overtime pay. The employee's pay and associated tax withholdings and records required correction in a subsequent paycheck after the employee reported this error to management.

Work unit staff incorrectly entered the employee's hours worked causing the error. Although the Payroll Department questioned the amount as unusual and provided guidance on the proper way to complete the form, management of the work unit did not provide a revised form prior to processing the payroll. Management of the business unit's confusion on how to properly complete the form led to the delay in providing the approved overtime hours to the Payroll Department until three pay periods after the employee worked the overtime.

Health should provide guidance on how to use the overtime form and clarify that managers should only enter the overtime hours worked as opposed to the total hours worked. In addition, Health should require that managers provide this information to the Payroll Department prior to the end of the following pay period for timely processing. This will reduce the risk of overpayments to salaried or classified employees who work overtime and will ensure timeliness of overtime payments to employees.

Why the APA Audits the Expense Allocation Process

Health spends over $640 million annually and allocates a large portion of these expenses across different funds based on amounts received in support of Health's programs. During fiscal year 2019, Health performed journal entries to allocate about $170 million between the general and special revenue funds. With a significant amount of expenses allocated this way, it is critical for Health to perform this process properly as an incorrect methodology risks misclassifying the expenses among these funds. To determine whether Health allocated these expenses and liabilities properly, we performed a re-calculation of the allocation percentages and compared them to the revenues received.

Improve the Expense Allocation Process

Type: Internal Control
Severity: Significant Deficiency
Repeat: No

Health did not properly allocate expenses among three different funds resulting in a misstatement of expenses at the end of the year. Health initially pays expenses from the general fund and later allocates the expenses among various special revenue funds based on the revenues received. At fiscal year-end, Health usually performs an analysis and makes a final "true-up" entry, but Health did not perform this analysis or make the final "true-up" entry at the end of fiscal year 2019.

CAPP Manual Topic 60104 defines the general fund as the fund which accounts for the ordinary operations of government and states that "all activities that do not qualify for inclusion in any other fund should be included in the general fund." The same section of the CAPP Manual states that a special revenue fund "accounts for activities, which are supported from revenues, derived from restricted taxes and other special revenue sources." Therefore, it is critical to properly match the expenses to the appropriate funding sources.

As a result of not properly allocating expenses, Health misclassified a total of $2,137,432 in expenses among three funds. At the end of fiscal year 2019, Health understated expenses in the Local Health District Match Fund by $2,137,432, overstated expenses in the Local Health District Service Fee Fund by $1,383,782, and overstated general fund expenses by $753,650. In addition, this error affected Health's year end leave liability submission to Accounts as Health uses these same percentages to allocate its leave liability. The leave liability information contained a misclassification between the same three funds totaling $108,479.

These errors were due to turnover in a key position within the General Accounting Department. The person responsible for evaluating whether the year-end "true-up" entry was necessary vacated her position prior to completing this task, and there was no backup person assigned. Additionally, there are no procedures in place outlining these key responsibilities.

Health should work with Accounts to determine if this misclassification requires an adjustment to its accounting records in fiscal year 2020. Additionally, Health should document all business-critical tasks in the General Accounting Department so that other people can perform these functions in the absence of the primary person. Finally, Health should designate a backup person to perform each of these tasks in cases where the primary person is unavailable. This will reduce the risk of missing key journal entries and ensure the correct allocation of expenses at year-end.

Why the APA Audits Hours Worked by Wage Employees

Health employs approximately 345 wage employees who are not eligible to participate in the state health insurance plan. Because of the financial penalties associated with violating federal laws pertaining to health insurance coverage, Health's management must take necessary precautions to prevent employees from exceeding allowable hours worked thresholds. To determine if these wage employees exceeded this threshold, we compared the hours worked by Health's wage employees to the hours allowed by the Affordable Care Act and the Virginia Acts of Assembly.

Develop and Implement Policy for Monitoring Part-time Employee Hours

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

Health does not adequately ensure part-time employees work less than an average of 29 hours per week, which equates to a total of 1,508 hours annually. For the look-back period from May 1, 2018, through April 30, 2019, Health had six part-time employees who averaged greater than 29 hours per week and, therefore, exceeded the 1,508-hour limit. Health has developed procedures to generate monthly monitoring reports and to notify departmental managers of part-time employees approaching 1,500 hours annually. However, Health should strengthen these procedures to require limiting the employees' hours after the Payroll Department sends out these notifications.

The Affordable Care Act requires certain employers to provide health care benefits to all full-time employees who work a weekly average of 29 hours or more. Additionally, Chapter 854 § 4-7.01g of the 2019 Virginia Acts of Assembly states that part-time Commonwealth employees may not work more than 29 hours per week on average over a twelve-month period. Health's internal procedures require the Payroll Department to send out warnings to managers advising that their employees are approaching 1,500 hours to prevent non-compliance with the state and federal regulations.

When the agency has part-time employees working the equivalent of full-time jobs without full-time job benefits, it could create the appearance of unequal treatment for those employees and could create future liabilities for the agency. By allowing a part-time employee to work more than an average of 29 hours per week for a year, Health is out of compliance with federal and state regulations and can be subject to penalties or even incur the costs of providing benefits to part-time employees.

Although the Payroll Department sent out warnings to managers indicating their employees were approaching the 1,500-hour limit outlined in the Payroll Department's procedures, management did not take action to limit the quantity of hours worked after this notification. Additionally, there are no specific actions outlined in Health's procedures that require the responsible supervisors to ensure compliance with the 1,500-hour rule.

Health should strengthen policies and procedures related to the monitoring of part-time hours. Health should document and implement a procedure specifically requiring managers to take action after reviewing the monitoring reports generated by the Payroll Department. Health's district managers should maintain an awareness of their part-time employees' total hours worked and reduce their hours as they approach the yearly limit. This will help to ensure compliance with the Affordable Care Act and the Virginia Acts of Assembly.

Why the APA Audits Compliance with the Conflicts of Interest Act

The purpose of the Conflicts of Interest Act is to ensure that public officers and employees fully represent the public interest as opposed to pursuing their own interests in the performance of their job responsibilities. When an agency places a public employee in a position where the employee stands to gain economically for services rendered within the scope of the employee's official duties, a conflict of interest exists. Properly disclosing any potential conflicts of interest helps agencies identify positions and responsibilities which they should not assign to certain employees. We compared Health's processes with the requirements established by the Conflicts of Interest Act to evaluate compliance.

Comply with the Conflicts of Interest Act
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Health did not require all employees designated as occupying positions of trust to complete the required Statement of Economic Interest (SOEI) training within the required timeframe. Pursuant to the Code of Virginia § 2.2-3130 (Conflicts of Interest Act), SOEI filers must complete orientation training to help them recognize potential conflicts of interest. Employees in positions of trust must complete this training within two months of hire and at least once during each consecutive period of two calendar years.

Thirty-four of 70 (48.6%) employees designated as required filers did not complete the training. By not ensuring that all required employees have completed the necessary training, Health may not be able to rely on its employees to effectively recognize, disclose, and resolve conflicts of interest.

Health's Shared Administrative Services (SAS) did not adequately monitor employees or hold them accountable for compliance with SOEI training requirements. Health relies on an automated notification system to inform new and existing employees when they must complete certain required

trainings and provides them with deadlines for completion. SAS did not properly include the SOEI Orientation within these notifications.

SAS should monitor all employees designated in positions of trust to ensure they complete the required SOEI training once within each consecutive period of two calendar years. SAS should update the notification system to include the SOEI Orientation and all other required trainings. This will reduce the rate of non-compliance with the Conflicts of Interest Act and reduce the risk of improper or incomplete conflicts disclosure.

Why the APA Audits the Financial Reporting Process

The Department of Medical Assistance Services' (Medical Assistance Services) payable and receivable accruals at year-end are material to the CAFR. As a result, it is important for Medical Assistance Services to have a thorough understanding of significant financial reporting policies and the information it provides to Accounts for inclusion in the CAFR. To evaluate Medical Assistance Services' year-end financial reporting process, we reviewed Medical Assistance Services' accrual methodologies and supporting documentation used to prepare the information submitted to Accounts.

Strengthen Controls over Year-End Accrual Reporting

Type: Internal Control
Severity: Material Weakness
Repeat: Yes (first issued in fiscal year 2018)

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

- Staff incorrectly classified a Private Hospital Enhanced Rate Payment liability, which resulted in a $139.2 million overstatement of the general fund claims payable liability and understatement of the Health Care Provider Payment Rate Assessment (Rate Assessment) fund claims payable liability. This error also impacted revenues and receivables in the Rate Assessment Fund.

- Staff incorrectly allocated the Medicaid expansion claims payable liability, which resulted in an $18.7 million overstatement of the federal fund claims payable liability and understatement of the Health Care Provider Coverage Assessment Fund claims payable liability.

- Staff's methodology for calculating an estimate of a Private Hospital Enhanced Rate Payment liability was inadequate, which resulted in a $19.6 million overstatement of the federal fund claims payable liability and the federal fund receivable. This also resulted in a $17.5 million overstatement of the Rate Assessment Fund claims payable liability.

- Staff misclassified a portion of the Family Access to Medical Insurance Security (FAMIS) claims payable liability, which resulted in a $15.8 million overstatement of the total Medicaid claims payable liability and understatement of the total FAMIS claims payable liability.

- Staff incorrectly recorded an adjusting journal entry to reverse prior year activity, which resulted in a $26.1 million understatement of revenues and expenses in both the general and federal funds.

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

As a result of these errors, Medical Assistance Services staff had to resubmit multiple pieces of information to Accounts causing inefficiencies for Medical Assistance Services' staff as well as delays for Accounts' staff. There are multiple factors that contributed to these errors. First, there were significant changes in operations due to Medicaid expansion, and Medical Assistance Services did not properly consider all of the financial reporting implications of these changes. In addition, there has been significant turnover in key positions in both the Fiscal Division and Budget Division, which has caused a lack of consistency in staff preparing this information from year to year. Finally, a lack of communication between the Fiscal Division, Budget Division, and Provider Reimbursement Division also contributed to some of these errors.

Medical Assistance Services should strengthen its controls over the preparation of year-end financial reporting information for Accounts. They should consider incorporating a technical supervisory review into the process given the complexity of the information to ensure significant errors are detected and prevented. As part of preparing the information, the Fiscal Division, Budget Division, and Provider Reimbursement Division should collaborate as needed to ensure there is a common understanding of significant financial reporting policies and that submitted information is accurate. Given the significance of Medical Assistance Services' financial activity, it is also important to consult with Accounts on financial reporting issues that may be complex or unusual to ensure both agencies have a thorough understanding of the nature of the activity and agree on the correct financial reporting treatment prior to submission of the information.

Improve Financial Reporting for Accounts Receivable
Type: Internal Control
Severity: Material Weakness
Repeat: No

Medical Assistance Services' Fiscal Division needs to improve its reporting and management of accounts receivable. Medical Assistance Services has outstanding accounts receivable due at any given time from various parties for fraud restitution, overpayments, and amounts due from third party providers, as examples. The Fiscal Division estimates a portion of these receivables as uncollectible for year-end financial reporting purposes and reports this to Accounts; however, the methodology for the

estimate is not formally documented. In addition, the methodology does not adequately consider the collectability of certain types of material receivables that are many years overdue, calling into question the soundness of the methodology and the accuracy of the estimate.

CAPP Manual Topic 20505 requires management to establish an allowance for doubtful accounts to reflect the amount of an agency's receivables that management estimates will be uncollectible. The method of establishing the allowance is left to the agency's discretion; however, the estimated allowance should be based upon historical data or other pertinent information relative to the receivables in question. Best practices also dictate that when accounting estimates are developed for financial reporting purposes, management is responsible for developing a sound methodology and documenting the basis for the methodology.

The lack of a sound and documented methodology for estimating uncollectible accounts impacts the accounts receivable information submitted to Accounts for year-end financial reporting. Given the age and amount of some of the receivables, it is likely the estimate is materially understated, which results in an overstatement of net accounts receivable. In addition, the lack of adequate documentation and data to support the methodology is also an issue in the event of employee turnover. In this case, turnover in the Accounts Receivable Manager position affected the Fiscal Division's ability to allocate the resources needed to perform a review of this area and update its policies, procedures, and methodology.

The Fiscal Division should review and evaluate its current methodology for estimating uncollectible accounts, giving consideration to the various types of accounts. This review should include a robust and detailed analysis of historical collection data by type of receivable, as well as age of receivable, to support a revised percentage estimate for accounts receivable that will not be collected. In addition, the Fiscal Division should update its policies and procedures over the accounts receivable area to ensure the financial accounting and reporting processes are adequately documented and the methodology for the allowance estimate is sufficiently supported.

Why the APA Audits Information Security

Medical Assistance Services' claims processing system is a critical information system that stores protected health information for over one million individuals and is used to process over $12 billion in medical claims annually. While the claims processing system is managed and operated by a third-party provider, Medical Assistance Services is the system owner and is responsible for ensuring the system is managed in accordance with the Security Standard. It is important for Medical Assistance Services to maintain oversight and gain assurance the provider has effective security controls to protect the confidentiality, integrity, and availability of data in the claims processing system. To evaluate Medical Assistance Services' management of information security, we compared internal control practices to those required by the Security Standard and reviewed the policies, procedures, and processes that support its third-party oversight process. We also evaluated Medical Assistance Services' controls for managing system access.

Complete and Approve the System Security Plan
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Medical Assistance Services does not have a complete and formally approved System Security Plan (SSP) with the vendor that manages the claims processing system. Medical Assistance Services has been working with the vendor to ensure they are in compliance with their contractual requirements and complete the SSP in response to findings from an external 2017 system security review. Medical Assistance Services continues to work with the vendor, but the SSP is not complete and multiple gaps remain between the vendor's controls and Medical Assistance Services' internal policies and procedures.

The contract between Medical Assistance Services and the vendor, Section 6.0 Security and Risk Assessment, states that the vendor will maintain a current SSP according to Medical Assistance Services' policies, procedures, standards, and guidelines. Additionally, 45 CFR § 95.621 requires the establishment of a security plan that addresses various system security requirements.

An SSP is important because it documents the minimum control requirements the vendor must implement to protect confidential and sensitive Commonwealth data. Without a complete SSP that has the formal approval of Medical Assistance Services and the vendor, the system may lack certain controls to protect the confidentiality, integrity, and availability of its mission essential data. Additionally, without a complete SSP, the roles and responsibilities between Medical Assistance Services and the vendor may be unclear, thereby increasing the risk of service disruption or data breach due to missing or ambiguous controls.

Medical Assistance Services did not meet its original due date, March 31, 2018, for completing the SSP because Medical Assistance Services is in the process of replacing the current system and the vendor has competing priorities with transitioning to the new system. Medical Assistance Services should complete the SSP and receive formal approval to ensure the vendor is meeting their contractual obligations. Medical Assistance Services should also ensure the SSP aligns with the requirements in its own policies, procedures, standards, and guidelines. Medical Assistance Services is unable to provide a specific completion date when the SSP will be complete and receive formal approval but has set a tentative goal of December 31, 2019.

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

Medical Assistance Services did not remove access to the claims processing system timely for individuals who no longer needed access. Five out of 12 (42%) employees did not have their system access disabled within 24 hours of separation, which occurred during the first six months of the fiscal year. These employees retained their system access between two and 27 days after separation. In

January 2019, Medical Assistance Services implemented a new process, but we continued to find issues with untimely removal of access. Two out of 12 (17%) employees who separated after January did not have their access terminated within 24 hours of separation. The employees retained access for five and 27 days after separation.

Additionally, one out of three (33%) employees did not have their access to the Commonwealth's accounting and financial reporting system disabled timely following a change in job responsibilities. The employee retained system access for 60 days after the change in job responsibilities.

Medical Assistance Services' IT Access Control AC-1 Policy Section A11 (b) (i) requires that "all user accounts must be disabled immediately upon separation or within 24 business hours upon receipt by the Office of Compliance and Security." This internal policy is not in agreement with the Security Standard Section PS-4, which states an organization must disable information system access within 24 hours of employee separation and terminate any authenticators or credentials associated with the individual. Not timely disabling access to a web-based mission critical system threatens the data integrity of the system. If separated employees retain access to the claims processing system and the Commonwealth's accounting and financial reporting system, users are potentially able to view, copy, and edit sensitive information.

Medical Assistance Services is not suspending separated employees' access in a timely manner due to ineffective and untimely communication within the agency. The new exit clearance workflow process must be initiated by the employee's supervisor in order for automatic notification to be sent to the Office of Compliance and Security (Compliance and Security) for removal of system access. There can also be differences in an employee's last day in office and his or her separation date, which contributed to some of these exceptions. Additionally, disabling access to the claims processing system requires input from multiple employees within Compliance and Security.

For removing access to the Commonwealth's accounting and financial reporting system, the process requires proper communication and manual approvals before access can be disabled. When combined with the issues noted above, the manual nature of the process often prevents timely removal of separated users. Lastly, Medical Assistance Services' current internal policy is not in compliance with the Security Standard, and prior approval for this deviation was not obtained from VITA.

Compliance and Security and the Human Resources Division should establish effective, regular communication to report staff changes to those individuals responsible for managing system access to ensure users' access is removed timely. In addition, Compliance and Security and the Human Resources Division should clarify its policy to ensure there is a consistent understanding of an employee's last day of employment and his or her separation date. Lastly, Compliance and Security should evaluate its internal policy to ensure it is clear and also consistent with the Security Standard. Any exceptions to the Security Standard requirements need to be approved by VITA.

Why the APA Audits Collection Efforts

Medical Assistance Services has several program integrity units that have the combined responsibility to identify suspected fraud, waste, and/or abuse across the Medicaid program. In cases where these units find that funds are to be returned, Medical Assistance Services has a set of procedures to follow to increase the likelihood that overpayments are collected. To evaluate collection efforts, we compared Medical Assistance Services' actions to its internal policies and procedures.

Continue Improving the Overpayment Collection Process

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2016)
Prior Title: Continue Improving the Accounts Receivable Collection Process

Medical Assistance Services' Accounts Receivable Unit needs to continue to improve its collection process for overpayments. Although improvements have been made in this area, they need to ensure that policies and procedures for collecting overpayments are followed. For two of nine (22%) overpayments identified by the Provider Review Unit, the Accounts Receivable Unit did not send invoice letters in a timely manner. These invoice letters were sent between two and seven days late based on the internal policy. There was one additional overpayment reviewed where the invoice letter was sent 150 days late, but this overpayment was less than one dollar, which brings into question the cost effectiveness of the collection policy.

Medical Assistance Services, to comply with the Virginia Debt Collection Act, Code of Virginia §2.2-4800-4809, established procedures to pursue collection of overpayments from recipients and providers. These procedures specify timeframes in which overpayment notice letters and invoicing letters must be sent to recipients and providers. For provider overpayments, the procedures require the Accounts Receivable Unit send an invoice letter to the provider 34 days from the date they receive notification from the Provider Review Unit. By not following established procedures designed to meet Commonwealth requirements, Medical Assistance Services is potentially not collecting money owed from providers or not collecting money owed to them timely.

There has been significant turnover in Accounts Receivable staff including the Accounts Receivable Manager position. This turnover, combined with the high volume of work, has contributed to the majority of the delays identified. The issue related to the immaterial overpayment was due to confusion over whether or not there is an internal policy that establishes a threshold for collection (i.e., the amount has to be over a certain dollar amount to pursue collection efforts).

Management should evaluate resources assigned to these areas to ensure they are adequate to perform the necessary functions in accordance with policies and procedures. In addition, Medical Assistance Services should evaluate its current policies in several areas. The Accounts Receivable Unit

should evaluate its internal policy over collections to determine whether it is appropriate to establish a dollar threshold to guide collections efforts. This will help to ensure resources are used in the most effective manner. In addition, the Accounts Receivable Unit may want to clarify its internal policy in terms of business days or calendar days.

Why the APA Audits Compliance with the Statement of Economic Interest Requirements

Medical Assistance Services has designated over one hundred employees in a position of trust. The Code of Virginia requires all individuals in a designated position of trust to complete the Statement of Economic Interest Disclosure Forms and the related training. To evaluate Medical Assistance Services' compliance with the Code of Virginia, we compared its practices to those required by the Code of Virginia.

Ensure Employees Complete Required Conflict of Interest Training

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

Medical Assistance Services did not ensure employees completed the required Conflict of Interest training within the timeframe outlined in the Code of Virginia. Specifically, 15 out of 138 (11%) employees who hold positions of trust did not complete the Conflict of Interest training within the required timeframe.

Pursuant to Code of Virginia § 2.2-3128 through § 2.2-3131, each state filer shall attend the orientation course within two months after he or she becomes a state filer and at least once during each consecutive period of two calendar years commencing on the first odd-numbered year thereafter. In addition, the Code of Virginia § 2.2-3129 requires agencies to keep a record of attendance that includes the specific attendees, each attendee's job title, and the dates of attendance for a period of not less than five years after each course is given.

Medical Assistance Services could be susceptible to actual or perceived conflicts of interest that would impair or appear to impair the objectivity of certain decisions made by employees in positions of trust. Additionally, not completing the Conflict of Interest orientation course may prevent Medical Assistance Services employees from recognizing or properly disclosing a conflict of interest.

Although the Human Resources Division has policies and procedures to guide management through the process of identifying employees for whom these requirements would be applicable, they had difficulties monitoring employees and holding them accountable for compliance with Conflict of Interest requirements due to the manual process. Medical Assistance Services is in the process of modifying the policies and procedures to require all state filers within the agency to complete the training every January, which will help the Human Resources division monitor employees who have not completed the training.

The Human Resources Division should ensure compliance with its internal policy and the Code of Virginia by monitoring all employees designated in a position of trust to ensure they complete the required Conflict of Interest training within two months of becoming a filer and once within each consecutive period of two calendar years thereafter. The Human Resources Division should also maintain a record of such attendance.

Why the APA Audits Compliance with Federal Requirements

The Department of Social Services (Social Services) spends almost two billion in federal dollars annually, with over 80 percent of these funds being passed through to a subrecipient. Not complying with the federal requirements for these funds could lead to the loss of federal funding. We reviewed Social Services' compliance with federal requirements for the following programs: Temporary Assistance for Needy Families (TANF), Foster Care, Adoption Assistance, Social Services Block Grant, and Community Services Block Grant. We also reviewed financial reporting and followed up on prior year findings for the Supplemental Nutrition Assistance Program (SNAP).

Improve Controls over SNAP Payments

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

Social Services does not have sufficient controls over payments made for SNAP. Social Services' case management system is used to determine who is eligible for SNAP and the benefit amounts. Social Services sends that information to a third-party vendor who gives the benefits to recipients via an Electronic Benefits Transfer (EBT) card and the vendor then draws down the funds from the federal government. The Division of Finance (Finance) completes a daily three-way reconciliation between Social Services' case management system, the vendor's system, and the federal payment system that is used to draw down federal funds. The reconciliation shows that the vendor's system and the federal payment system had approximately $234 million more benefits given during fiscal year 2019 than the case management system reflects. In addition, this reconciliation is not reviewed or approved by a supervisor.

Social Services' Division of Enterprise Systems (Enterprise Systems) and Finance did not resolve the discrepancies between the systems and; therefore, could not provide support for $234 million out of $1,013 million (23%) that was paid out by the vendor and drawn down from the federal government. Finance also used the amount paid out by the vendor when reporting revenue and expenditure amounts for the SNAP program to Accounts for use in the CAFR. Finally, while Social Services was relying on the vendor's system to provide reporting for the CAFR, Social Services was not maintaining proper oversight of this vendor, see management recommendation entitled "Develop a Process to Maintain Oversight for Third-Party Providers" for more information on this issue. After we brought this issue to management's attention, Finance and Enterprise Systems were able to work together to provide evidence that the total amount authorized by the case management system reasonably agreed to the total amount the vendor put on the EBT cards.

2 CFR § 200.303(a) states that an entity must establish and maintain effective internal control over federal awards that provides reasonable assurance that the entity is managing the award in compliance with the federal statutes, regulations, and terms and conditions of the federal award. As an internal control, a supervisor should review each reconciliation and its support to ensure it is properly

supported and accurate. In addition, 7 CFR § 247.4 states that state agencies shall reconcile total funds entered into, exiting from, and remaining in the EBT system each day.

Finance did not investigate and resolve the discrepancies between Social Services' case management system, amounts given to recipients, and drawn down from the federal government because there were known problems with the case management system that have not been addressed by Enterprise Systems. Without adequate controls over the reconciliation process requiring approvals, identifying and resolving discrepancies, and ensuring proper support for amounts drawn down from the federal government, it could create questions as to whether the nature of the payments are permissible and could lead to potential disallowed charges by the federal government. Additionally, by not addressing discrepancies noted during the reconciliation process, Finance increases the risk of inaccurate data being reported in the CAFR. We consider this a material weakness in internal control.

Finance and Enterprise Systems should work together to investigate and resolve the reconciling amounts and maintain appropriate documentation for all payments and amounts drawn down from the federal government. Finance should implement controls over the SNAP daily reconciliation to ensure data is accurate, discrepancies are resolved timely, documentation of supervisor's review and approval, and supporting documentation is maintained.

Improve Controls over Income Verification for the TANF Program

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)
Prior Title: Improve Controls over Income Verification for the Temporary Assistance for Needy Family Program

Social Services is still working on implementing a control to ensure the Income Eligibility and Verification System (IEVS) is used when determining eligibility for TANF participants. 45 CFR § 205.55 requires agencies to collect income information through IEVS. By not ensuring that IEVS is used when verifying income for TANF participants, Social Services cannot verify that participants in the TANF program have met all eligibility requirements.

Social Services submitted a change request to Enterprise Systems to design and implement a defined process for working the IEVS matches. The design for the new process for IEVS has been completed; however, it has not been implemented and is planned for implementation in calendar year 2020.

Social Services should continue implementation of the new IEVS process for local agencies processing TANF applications in order to utilize IEVS for verifying income. In addition, Social Services should implement a control to ensure that IEVS is utilized when determining eligibility for TANF.

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

Finance does not have adequate controls in place to ensure accurate federal quarterly reporting on the FNS-209 "Status of Claims Against Households" Report (FNS-209). Two FNS-209 reports reviewed identified the following:

- For one FNS-209 quarterly report, Finance could not provide documentation from the case management system to validate all the line items reported.

- For one FNS-209 quarterly report, Finance could not provide documentation from the case management system validating the beginning and ending balance line items.

7 CFR § 273.18 (m) requires agencies to maintain a system for monitoring recipient claims against households that maintains claims records and corresponding receivable information. The system must also be able to produce summary reports and reconcile to supporting records. Reporting potentially inaccurate or incomplete information prevents the United States Department of Agriculture, Food and Nutrition Service from adequately monitoring the status of claims against households.

Finance and Enterprise Systems have been working to address the system deficiencies in the case management system to ensure FNS-209 can be adequately supported; however, the beginning and ending balances reported on the FNS-209 report do not agree to the case management system. When Enterprise Systems performs a data fix to the case management system, it will alter the amounts in the system and any previously submitted FNS-209 reports are no longer adequately supported. In addition, Social Services does not have sufficient policies and procedures over the FNS-209 reporting process.

Finance and Enterprise Systems should continue to work together to ensure all information submitted in the FNS-209 can be sufficiently validated. Finance should create policies and procedures over the reporting process to ensure accurate reporting of claims against households.

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

Social Services does not have adequate controls in place to ensure accurate federal reporting for two TANF performance reports, the ACF-199 "TANF Data Report" and ACF-209 "SSP-MOE Data Report." These reports are submitted quarterly and utilize a case management system to create the reports. During our review, we identified the following discrepancies in four key line items, where key line items did not agree to information maintained in the case management system:

- Nine out of 50 (18%) cases did not properly report the *Receives Subsidized Child Care* key line item.

- One out of 25 (4%) cases did not properly report the *Toward Federal Time-Limit* key line item.

- Six out of 50 (12%) cases did not properly report the *Work Participation Status* and *Unsubsidized Employment* key line items. One of the cases was the result of the key line items not agreeing to information maintained in the case management system. The five remaining cases did agree to the information in the case management system; however, the information in the system was entered incorrectly by the local Department of Social Services.

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, data is free of computational errors, and is internally consistent. Reporting potentially inaccurate or incomplete information prevents the Administration for Child and Families from adequately monitoring Social Services' work participation rates and overall performance for the TANF program. In addition, if Social Services is found to not be meeting minimum work participation rates, a penalty can be imposed on the awarded grant. These reporting errors can be attributed to the implementation of the case management system. Social Services should continue working with Enterprise Systems to correct system deficiencies to ensure all information submitted in federal reports is accurate.

Ensure Subrecipient Reviews Adhere to Monitoring Plan
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)

Social Services is still not adhering to its established approach for monitoring subrecipients. The established approach includes having the Division of Community and Volunteer Services (Community and Volunteer Services) exercise agency wide oversight over the subrecipient monitoring process to ensure the various divisions are following the established monitoring plans and produce reports to consolidate the monitoring activity agency wide. During fiscal year 2019, Social Services did not produce quarterly reports to brief Executive Management on subrecipient monitoring activities for each Division within Social Services.

2 CFR § 200.331(d) requires pass through entities to monitor the activities of subrecipients as necessary to ensure that the sub-award is meeting grant requirements. To aid in this process and mitigate risk, Social Services develops annual monitoring plans across divisions which outline the review process and reports the results of the reviews to executive management quarterly.

Without providing reports to executive management, we are not able to determine if Social Services is assessing each of their division's completed subrecipient reviews and if executive management is acting upon possible deviations from the plan. During fiscal year 2019, Social Services underwent a reorganization and created a new Compliance Division. The oversight for the agency's

overall subrecipient monitoring transitioned from Community and Volunteer Services to the Compliance Division. The Compliance Division is in the process of hiring a subrecipient monitoring manager and developing a subrecipient monitoring oversight process.

Social Services should ensure that all divisions are adhering to the established approach for monitoring subrecipients. Specifically, Social Services should work to ensure progress reports are provided to executive management for review and monitoring of subrecipients.

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

Social Services continues to not provide assurance that audits are performed and reviewed for all subrecipients expending $750,000 or more and that management is making timely decisions based on the results of the audit report reviews. Community and Volunteer Services is responsible for reviewing non-profit organization audit reports and the Local Review Team is responsible for reviewing locality audit reports. Our testwork identified the following:

- Five of 17 (29%) non-profit organizations expending more than $750,000 tested had not been reviewed by Community and Volunteer Services, to determine if proper audits were completed, at the time of our audit. Three of the five organizations selected for testwork were not included on the non-profit audit report tracking spreadsheet until it was brought to Community and Volunteer Services' attention during our audit.

- Reports to senior management and regional directors, detailing the results of the locality and non-profit organization audit report reviews to be used in issuing official management decisions to subrecipients, have not been issued by the Local Review Team or Community and Volunteer Services.

According to 2 CFR § 200.331 (f), pass thru entities are required to verify that every subrecipient is audited as required. 2 CFR § 200.501(a-b) requires all non-Federal entities that expend $750,000 or more during the non-Federal entity's fiscal year in Federal awards must have a single or program-specific audit conducted for that year. 2 CFR § 200.512 requires audit reports be submitted within the earlier of 30 days after receipt of the auditor's report or nine months after the end of the audit period. Additionally, 2 CFR § 200.521 requires pass-through entities to issue management decisions within six months of acceptance of the audit report.

Without maintaining a complete listing of all non-profit organizations required to have an audit and reviewing all of those audit reports, Community and Volunteer Services is unable to provide assurance that it is meeting the audit requirements set by the federal regulations. Additionally, without providing senior management and regional directors the results of the audit report reviews timely, management cannot make decisions within the timeframes set by the federal regulations.

Community and Volunteer Services attributed the incomplete tracking spreadsheet for non-profit reviews to competing priorities and difficulty in obtaining all audit reports. Social Services plans to transition the review of non-profit organization audit reports from Community and Volunteer Services to the newly established Compliance Division in fiscal year 2020. Additionally, review results have not been reported to senior management and regional directors because Community and Volunteer Services and the Local Review Team want all non-profit and locality audit reports to be received and all reviews to be completed prior to reporting results.

Social Services should ensure that all subrecipients are monitored in accordance with all federal requirements. Additionally, Social Services should develop a process to ensure that senior management and other responsible parties are notified timely of the results of the audit reviews so that prompt and meaningful management decisions can be issued in accordance with federal requirements.

Ensure Family Services Subrecipient Reviews Adhere to Monitoring Plan

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

Social Services' Division of Family Services (Family Services) cannot provide assurance that Adoption Assistance and Title IV-E Foster Care subrecipient monitoring reviews are completed timely and in accordance with Family Services' subrecipient monitoring plan and related processes. Our testwork over 25 Adoption Assistance and IV-E Foster Care monitoring reviews identified the following:

- For four Adoption Assistance reconciliation reviews tested, there was no communication notifying the local agency the review was complete and if variances were identified in accordance with Family Services' established monitoring process.

- For one Adoption Assistance reconciliation review tested, variances were identified by the assigned Quality Assurance and Accountability (QAA) consultant in October 2018, and the variances have not been resolved, over one year later.

- For one IV-E Foster Care Training monitoring review tested, all documentation supporting the QAA consultant's assessment and conclusions was not provided.

2 CFR § 200.331(d) requires pass through entities to monitor the activities of subrecipients as necessary to ensure that the sub-award is meeting grant requirements. To aid in this process and mitigate risk, Family Services develops an annual monitoring plan, which outlines the review process. Without maintaining adequate support and resolving identified issues timely, Family Services cannot provide assurance that it is completing subrecipient monitoring reviews in accordance with its monitoring plan and federal guidelines.

Family Services implemented the process of communicating the results of its Adoption Assistance reconciliation reviews in February 2018; however, Family Services stated that during fiscal year 2020

they were able to streamline and improve the process. Additionally, the consultant that completed the IV-E Foster Care Training monitoring review separated from Social Services and the evidence supporting the consultant's assessments was not retained and/or accessible by Family Services.

Family Services should ensure that all consultants are performing reviews as outlined by the monitoring plan and internal processes. Additionally, Family Services should ensure that reviews are being completed timely and adequate documentation is maintained supporting the reviews.

Why the APA Audits Information System Security

Social Services is responsible for managing numerous social programs for the Commonwealth of Virginia, such as TANF, SNAP, Foster Care, and Child Support Services. In order to manage the significant volume of personal and financial data, Social Services relies on information technology (IT) systems for the collection, management, and storing of data. Due to the sensitivity of the data, appropriate policies, procedures, and security controls in accordance with the Security Standard, federal regulations, and industry-specific best practices must be in place to ensure its protection from malicious intent and disastrous events. To evaluate the controls surrounding information systems, we compared the practices of Social Services to those required by the Security Standard.

Social Services also manages eligibility for the Medicaid program on behalf of Medical Assistance Services. Eligibility for Medicaid is managed using Social Services' case management system. Therefore, the IT recommendations below could have an effect on the Medicaid program.

Continue Improving IT Risk Management Program

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

Social Services continues to improve its IT Risk Management documentation. Since the prior year audit, Social Services completed its annual test of the Continuity of Operations Plan and four IT System and Data Sensitivity Classifications. However, Social Services does not comply with the following areas:

- Social Services does not have documentation supporting the IT System and Data Sensitivity Classifications for one system (2.5%) out of a total of 40 sensitive systems. The Security Standard, Section 4, requires Social Services classify the IT system as sensitive if any type of data handled by the system is sensitive based on confidentiality, integrity, or availability.

- Social Services does not have IT System Risk Assessments for three systems (7.5%). The Security Standard, Section 6.2, requires the agency to conduct and document a risk assessment for each IT system classified as sensitive at least once every three years.

- Social Services does not have System Security Plans for two systems (5%). The Security Standard, Section PL-2-COV, requires Social Services document a System Security Plan for the IT system.

- Social Services does not perform annual reviews of its Risk Assessments and System Security Plans to determine the continued validity of the documents. The Security Standard, Section 6.2, requires Social Services conduct an annual self-assessment of the Risk Assessment, and Section PL-2 requires the agency to review the System Security Plans on an annual basis or more frequently to address environmental changes.

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

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

Social Services had a reorganization of executive positions under the Commissioner that included hiring a new Deputy Commissioner of Information Management and Technology. The new Deputy Commissioner of Information Management and Technology was reorganizing the four information technology divisions that report to the new position, which included the divisions of Information Systems, Enterprise Systems, Information Security and Risk Management, and Data Management. Part of the reorganization included a new Risk Manager position that will be responsible for developing and updating Social Services' IT Risk Management and Contingency Planning documentation. The Deputy Commissioner of Information Management and Technology left the agency in October 2019, putting the reorganization and filling the Risk Manager position on hold.

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

Continue Improving Database Security

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

Social Services continues to not perform certain security procedures over the databases supporting its financial reporting system and case management system in accordance with the Security Standard and industry best practices. We communicated the weaknesses for both systems to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

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

Social Services should dedicate the necessary resources to ensure that database procedures and controls align with the requirements in the Security Standard. Additionally, Social Services should consistently implement controls across all of its systems. Doing this will help maintain the confidentiality, integrity, and availability of sensitive and mission critical data.

Develop Records Retention Requirements and Processes for Case Management System

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

Social Services did not make progress to develop and implement electronic records retention requirements for its case management system. We communicated the deficiencies 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.

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

Retaining records longer than necessary causes the Commonwealth to spend additional resources to maintain, back-up, and protect the information. Additionally, without documenting and implementing records retention requirements, Social Services may not be able to ensure that backup and restoration efforts will provide mission essential information according to recovery times. Social Services placed corrective actions on hold due to competing priorities of Medicaid expansion and other corrective actions within the IT environment. Social Services' goal is to develop and implement record retention requirements in November 2020.

Social Services should identify retention requirements for the data within its case management system. Additionally, Social Services should implement a process, whether a manual process or automated control, to ensure consistent compliance with the retention requirements the agency identifies for each data set within the IT system.

Develop a Process to Maintain Oversight for Third-Party Providers

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

Social Services does not have a formal process to manage its third-party Software as a Service (SaaS) providers that fall under VITA's Enterprise Cloud Oversight Service (ECOS). Social Services uses VITA's ECOS to assist the agency with gaining assurance that its SaaS providers implement the minimum security requirements required by the Commonwealth's Hosted Environment Information Security Standard, SEC 525 (Hosted Environment Security Standard).

Specifically, Social Services does not have any policies or procedures that assign roles and responsibilities to ensure the correct employees, such as contract administrators or system owners, work with VITA's ECOS to receive and review communications from the SaaS providers. Additionally, Social Services does not have procedures or a process to ensure VITA's ECOS communicates with its SaaS providers to resolve weaknesses that are identified in the SaaS providers' independent audit reports. As a result, the SaaS provider that hosts Social Services' electronic benefits processing system and administers electronic payment of benefit cards for benefit programs such as SNAP, TANF, and Child Support received a qualified opinion in its two most recent independent audit reports and neither Social Services nor VITA's ECOS performed any follow-up with the SaaS provider to determine if they are properly remediating the weaknesses.

Executive branch agencies, such as Social Services, that receive IT services from VITA must follow the Third-Party Use Policy, which requires agencies to receive written approval from VITA prior to procuring, signing, or engaging with a third-party hosted (cloud) service, specifically SaaS providers. Social Services signed a Memorandum of Understanding (MOU) with VITA's ECOS that requires Social Services to review and approve all documentation evidencing VITA ECOS' performance of services to monitor compliance with the MOU. Additionally, the Hosted Environment Security Standard, Section 1.1, states management remains accountable for maintaining compliance with the Hosted Environment Security Standard through documented agreements and oversight of services provided.

Without a formal process to review and maintain VITA ECOS' documentation, Social Services cannot validate whether its SaaS providers implement security controls that meet the requirements in the Hosted Environment Security Standard to protect the agency's sensitive and confidential data. Social Services was unaware of its oversight responsibilities in the MOU for VITA's ECOS, which led to the weaknesses described above.

Social Services should develop a formal process to monitor and maintain oversight of its third-party SaaS providers to ensure they comply with the Hosted Environment Security Standard and that VITA's ECOS is meeting all requirements in the MOU. Doing this will help maintain the confidentiality, integrity, and availability of sensitive and mission critical data.

Improve Web Application Security

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

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

Social Services should develop a plan to implement the controls discussed in the communication marked FOIAE in accordance with the Security Standard in a timely manner. Doing this will help to ensure Social Services secures the web application to protect its sensitive and mission critical data.

Improve IT Change and Configuration Management Process

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

Social Services does not follow an IT change and configuration management process that includes all elements required by the Security Standard. Change management is a key control to evaluate, approve, and verify configuration changes to security components.

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

Social Services should develop a plan to implement the controls discussed in the communication marked FOIAE in accordance with the Security Standard in a timely manner. Improving Social Services'

IT change and configuration management processes will decrease the risk of unauthorized modifications to sensitive systems and help maintain the confidentiality, integrity, and availability of sensitive and mission critical data.

Improve Access Controls to Critical Systems
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2018)
Prior Title: Remove Separated Employees' Access to Critical Systems in a Timely Manner

Social Services does not have sufficient controls in place to ensure system access to critical systems is reasonable. Our review of user access across six critical systems identified the following:

- One new user was granted access permissions to Social Services' financial system in excess of the employee's job responsibilities;
- Three users were granted conflicting access to the Social Services' financial system;
- Two terminated employees retained access to Social Services' financial system;
- Two terminated employees retained access to Social Services' central security system;
- One terminated employee retained access to the Commonwealth's accounting and financial reporting system;
- Six terminated contractors retained access to the Social Services' childcare system;
- One active user to the Social Services' childcare system has two user login IDs, with different access for each ID;
- Three terminated employees retained access to the Commonwealth's human resource system; two of the three had their access for over a year after employment termination; and
- Seven employees had unnecessary access privileges based on their job responsibilities to the Commonwealth's retirement benefits system.

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

requires the agency to employ the principle of least privilege, allowing only authorized access for users that is necessary to accomplish assigned tasks.

Social Services does not have sufficient policies and procedures in place to ensure access is granted based on least privilege, access is removed timely, accurate based on conflicting access roles, and periodic reviews of access are completed. Additionally, the Separation and Transfer Checklist form does not include the Commonwealth's accounting and financial reporting system; therefore, the Security Officer did not receive notification to terminate access. Not communicating when an employee terminates and not conducting adequate access reviews to critical systems threatens the integrity of the system and data housed within the system, and allows employees with unapproved access, which increases the risk of compromising confidentiality of Social Services' critical data.

Social Services should update policies and procedures to reflect the requirements in the Security Standard. This would include ensuring access is granted based on the principal of least privilege, access is removed timely, and access does not involve conflicting roles. Social Services should update the Separation and Transfer Checklist form to include all systems and ensure there is proper communication with the Security Officer when there is a change with system access. Social Services should perform an annual access review of the critical systems and retain documentation of this review.

Why the APA Audits Compliance with the Conflict of Interests Act

Social Services has designated over 20 employees in a position of trust and some of these employees negotiate and award multi-million dollar contracts on behalf of the Commonwealth. The Code of Virginia requires all individuals in a designated position of trust to complete the Statement of Economic Interest Disclosure Forms and complete the related training. To evaluate Social Services' compliance with the Code of Virginia, we compared its practices to those required by the Code of Virginia.

Ensure Compliance with Conflict of Interests Act

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2017)
Prior Title: Ensure Statement of Economic Interest Filers Complete Required Training

Human Resources did not properly identify all employees and board members holding a position of trust, to ensure required disclosures were properly filed. Additionally, Human Resources did not ensure all employees in a position of trust completed the required Conflict of Interests Act (COIA) training timely. Our review identified the following:

- Human Resources did not identify two employees within Procurement as needing to file disclosures.

- Human Resources did not identify eight board members as needing to file disclosures.

- Seven out of 24 (29%) employees identified by Human Resources within a position of trust did not complete COIA training within two months of their hire date.

Per the Code of Virginia § 2.2-3114, persons occupying positions of trust within state government or non-salaried citizen members of policy and supervisory boards shall file a disclosure statement with the Commonwealth's Ethics Advisory Council annually. Additionally, per Executive Order Number Eight (2018), positions of trust for Executive Branch Agencies include, but are not limited to, Chief Procurement Officers and other positions with the ability to authorize and make contract and procurement decisions. The Code of Virginia § 2.2-3128 through § 2.2-3131 requires that each employee within a position of trust complete COIA training within two months of their hire date and at least once every two years after the initial training. This training is designed to help employees recognize potential conflicts of interest. The Commonwealth offers in-person and web-based training, which satisfies this requirement.

Without appropriately identifying positions of trust and ensuring those employees are completing the required training, Social Services could be susceptible to actual or perceived conflicts of interest and may be limited in its ability to hold its employees accountable for not knowing how to recognize a conflict of interest and how to resolve it. Additionally, employees and board members could be subject to penalties for inadequate disclosure on their filings, as outlined within the Code of Virginia § 2.2-3120 through § 2.2-3127. Human Resources updated their policies and procedures to meet Code of Virginia requirements for the COIA training; however, Human Resources misinterpreted the training requirement under the Code of Virginia and employees were provided incorrect instructions for completing the training within two months of hire date.

Human Resources should ensure employees within a position of trust and board members are appropriately identified and are provided adequate instruction and notice to maintain compliance with the COIA. Additionally, Human Resources should ensure that policies and procedures are updated to reflect current Code of Virginia requirements and the guidance issued by the Commonwealth's Ethics Advisory Council.

Why the APA Audits Compliance with Employment Eligibility Guidelines

Social Services employs over 1,600 employees. Noncompliance with federal government employment eligibility guidelines could result in financial penalties. To determine compliance with the employment eligibility process, we reviewed Social Services' processes and forms used to verify both employment eligibility and identity. We compared their processes to those required by the federal government and the Code of Virginia.

Continue to Improve Internal Controls over Employment Eligibility Verification Process
Type: Internal Control and Compliance
Severity: Deficiency
Repeat: Yes (first issued in fiscal year 2018)
Prior Title: Improve Processes and Controls over Employment Eligibility

Human Resources does not have sufficient internal controls over the employment eligibility verification process. Human Resources updated the policy manual to include all required employment eligibility practices; however, Human Resources continues to not complete employment eligibility verification forms in accordance with guidelines issued by the United States Department of Homeland Security. Human Resources could not provide the Form I-9 for two of the 32 employees (6%) randomly selected for testing. Of the remaining 30 employees tested, we noted the following deficiencies:

- For one employee (3%), Section 1 of the Form I-9 was not completed timely, on or before the first day of employment;

- For two employees (7%), Section 2 of the Form I-9 was not fully completed and was not completed timely, within three days of the first day of employment.

The Immigration Reform and Control Act of 1986 requires employers to verify employee's identity and employment authorization of each person they hire, complete and retain a Form I-9, Employment Eligibility Verification, for each employee. Per the Handbook for Employers M-274, issued by the United States Citizenship and Immigration Services (M-274), Forms I-9 must be retained for a period of at least three years from the date of hire or for one year after employee's employment termination, whichever is longer. The United States Citizenship and Immigration Services sets forth federal requirements for completing the Form I-9 in M-274.

Not complying with federal regulations could result in civil fines and/or criminal penalties and debarment from government contracts. By not performing due diligence with regard to Form I-9s as required by the Immigration Reform and Control Act of 1986, Human Resources is in noncompliance with federal regulations. Due to the high turnover in the Human Resources Department during fiscal year 2019, management did not ensure all employees received proper training, nor did management communicate federal government requirements in regards to employment eligibility verification process.

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

Why the APA Audits an Agency's Controls Over their Information in the Commonwealth's Retirement Benefits System

The Commonwealth's retirement benefits system is used to calculate total pension liabilities for the Commonwealth. Individual agencies are responsible for updating the records within the retirement benefits system related to their employees. As a result, Social Services' management must take adequate precautions to ensure the integrity of these records. To determine if management implemented these precautions, we compared the practices of Social Services to the guidance provided by Accounts and VRS.

Continue to Improve Reconciliation Process of the Commonwealth's Retirement Benefits System

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

Human Resources does not sufficiently reconcile retirement contributions before confirming to VRS that retirement data is correct. Human Resources confirmed retirement contributions before reconciling the data for 11 of 12 (92%) months for fiscal year 2019. In addition, Human Resources continued to not have sufficient monthly reconciliations between the Commonwealth's retirement benefits system and the Commonwealth's human resource system during fiscal year 2019. We noted all three (100%) monthly reconciliations randomly selected for review were incomplete, as they did not include the following:

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

CAPP Manual Topic 50410 requires agencies to confirm retirement contributions by the 10th of the following month in order to maintain compliance with the deadline and procedures established by VRS and states that employers are responsible for ensuring valid values are in the Commonwealth's retirement benefits system prior to confirmation of the contribution snapshot. Agencies must identify exception items on the Automated Reconciliation Reports and communicate them to the proper system of authority for correction, as soon as possible but no later than 31 days from the date of the report.

Improper pre- and post- certification processes can affect the integrity of the information in the Commonwealth's retirement benefits system that determines pension liability calculations for the entire

Commonwealth and can result in a misstatement in the Commonwealth's financial statements. Inadequate reconciliations can cause errors in members' retirement related data and can cause under or overpaying retirement contributions to the Commonwealth's retirement benefits system, which can create complications when members retire. Due to high turnover and lack of policies and procedures in the Human Resources Division, staff did not perform the reconciliation between the Commonwealth's retirement benefits system and the Commonwealth's human resource system adequately and prior to confirming the snapshot.

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

Why the APA Audits the Commonwealth's Human Resource System

Social Services uses the Commonwealth's human resource system to input personnel and compensation data that then drives payments to employees. Social Services had payroll expenses that exceeded $145 million during the fiscal year. Social Services' management must implement adequate controls to ensure the integrity of human resource data to ensure that payments to employees are accurate. To determine if controls over the human resource system were adequate we compared the practices of Social Services to those required by the CAPP Manual.

Improve Internal Controls over Commonwealth's Human Resource System

Type: Internal Control
Severity: Deficiency
Repeat: No

Human Resources does not have sufficient controls in place to ensure data in the Commonwealth's human resource system is accurate. Human Resources could not provide supporting documentation for the review of exceptions between the Commonwealth's human resource system and the Commonwealth's payroll system. Without retaining this documentation, there is no evidence that exceptions were reviewed and addressed.

CAPP Manual Topic 50410 requires agencies to reconcile human resource data to payroll data prior to the payroll certification deadline each pay period. CAPP Manual Topic 21005, Records and Retention, states that agencies should develop and implement procedures, guidelines, systems, and business practices that facilitate the creation, backup, preservation, filing, storage, and disposal of records of all formats. Moreover, CAPP Manual Topic 21005 outlines the minimum record retention periods for audit support, including all records relating to payroll. Accounts and the Library of Virginia established the minimum retention period for payroll files at five years or whenever audited, whichever is longer.

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

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 13, 2019

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Thomas K. Norment, Jr.
Chairman, Joint Legislative Audit
and Review Commission

We have audited the financial records and operations of the **Agencies of the Secretary of Health and Human Resources,** as defined in the Audit Scope and Methodology section below, for the year ended June 30, 2019. We conducted this performance audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, in support of the Commonwealth's Annual Financial Report and Single Audits. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Objectives

Our audit's primary objective was to evaluate the accuracy of the Agencies of the Secretary of Health and Human Resources' financial transactions as reported in the Comprehensive Annual Financial Report for the Commonwealth of Virginia for the year ended June 30, 2019 and test compliance for the Single Audit. In support of this objective, we evaluated the accuracy of recorded financial transactions in the Commonwealth's accounting and financial reporting system, in each agency's accounting records, and supplemental information and attachment submissions to the Department of Accounts; reviewed the adequacy of their internal control; tested for compliance with applicable laws, regulations, contracts, and grant agreements; and reviewed corrective actions of audit findings from prior year reports.

Audit Scope and Methodology

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

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

Department of Behavioral Health and Developmental Services

- Accounts receivable
- Acquisitions and contract management
- Commonwealth's retirement benefit system
- Community Service Board contracts
- Federal revenues, expenses, and compliance for:
  - Prevention and Treatment of Substance Abuse Block Grant
  - Opioid STR/SOR Grant
- Information system security
- Institutional revenues
- Licensing behavioral health providers
- Operational expenses
- Payroll expenses
- Systems access controls

Department of Health

- Accounts payable
- Accounts receivable
- Collection of fees for services
- Commonwealth's retirement benefit system
- Cooperative agreements between Health and local governments, including:
  - Accounts payable
  - Aid to and reimbursement from local governments
  - Cost allocations
- Federal revenues, expenses, and compliance for:
  - HIV Formula Care Grant
  - Immunization Cooperative Agreement
  - Special Supplemental Nutrition Program for Women, Infants, and Children
- Information system security
- Inventory
- Payroll expenses
- Rescue squad support
- Systems access controls

Department of Medical Assistance Services

- Accounts payable
- Accounts receivable

Contract management
Federal revenues, expenses, and compliance for:
    Medicaid Cluster
Provider assessment revenues
System access controls

Department of Social Services

Accounts payable
Accounts receivable
Budgeting and cost allocation
Child Support Enforcement additions and deletions
Eligibility for the following programs:
    Child Care and Development Fund
    Low Income Heating and Energy Assistance
Federal revenues, expenses, and compliance for:
    Adoption Assistance
    Community Services Block Grant
    Foster Care
    Social Services Block Grant
    Temporary Assistance for Needy Families
Network and system security
Subrecipient monitoring
Supplemental Nutrition Assistance Program supplemental information
Systems access controls

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

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

We performed audit tests to determine whether the agencies' controls were adequate, had been placed in operation, and were being followed. Our audit also included tests of compliance with provisions of applicable laws, regulations, contracts, and grant agreements. Our audit procedures included inquiries of appropriate personnel, inspection of documents, records, and contracts, and

observation of the agencies' operations. We performed analytical procedures, including budgetary and trend analyses. We also tested details of transactions to achieve our objectives.

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

Our consideration of internal control over financial reporting and compliance was for the limited purpose described in the section "Audit Objectives" and was not designed to identify all deficiencies in internal control over financial reporting 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 entitled "Internal Control and Compliance Findings and Recommendations," we identified deficiencies in internal control that we consider to be material weaknesses and significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements or noncompliance on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements or material noncompliance with a type of compliance requirement of a federal program will not be prevented, or detected and corrected on a timely basis. 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 explicitly identified 58 findings in the sections titled "Internal Control and Compliance Findings and Recommendations" as significant deficiencies and or material weaknesses for the Commonwealth.

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

Conclusions

We found that after adjustments, Medicaid Assistance Services properly stated, in all material respects, the amounts recorded and reported in the Commonwealth's accounting and financial reporting system, in the agency's accounting records, and in other financial information reported to the Department of Accounts.

We found that the remaining Agencies of the Secretary of Health and Human Resources, as defined in the Audit Scope and Methodology section above, properly stated, in all material respects, the

amounts recorded and reported in the Commonwealth's accounting and financial reporting system, in each agency's accounting records, and in other financial information reported 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 entitled "Internal Control and Compliance Findings and Recommendations."

The Agencies of the Secretary of Health and Human Resources have taken adequate corrective action with respect to audit findings reported in the prior year that are not referenced as "repeat" findings in the section titled "Internal Control and Compliance Findings and Recommendations."

Since the findings noted above include those that have been identified as material weaknesses and significant deficiencies, they will be reported as such in the "Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of the Financial Statements Performed in Accordance with Government Auditing Standards" and the "Independent Auditor's Report on Compliance for Each Major Federal Program; Report on Internal Control over Compliance; and Report on Schedule of Expenditures of Federal Awards Required by Uniform Guidance," which are included in the Commonwealth of Virginia's Single Audit Report for the year ended June 30, 2019. The Single Audit Report will be available at www.apa.virginia.gov in February 2020.

Exit Conference and Report Distribution

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

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.

Martha S. Mavredes
AUDITOR OF PUBLIC ACCOUNTS

LCW/clj

COMMONWEALTH of VIRGINIA

ALISON G. LAND, FACHE
COMMISSIONER

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

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

January 17, 2019

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

Dear Ms. Mavredes:

We have reviewed your report on our audit for the year ended June 30, 2019. We concur with the findings and our corrective action plan has been provided separately.

Regarding APA's Comment to Management, the Department of Behavioral Health and Developmental Services (DBHDS) began addressing this oversight concern with significant changes to the organizational structure in the summer of 2018. Virginia is facing unprecedented changes in the way behavioral health and developmental disability services are delivered, and the goal of restructuring was to allow DBHDS leaders to have a span of control that is manageable and supports operations, support how services will be delivered in the future, and add capacity to properly oversee evolving programs and services. One part of the reorganization that specifically addresses the Comment to Management was removing silos in administrative functions and creating an Administrative Services Division to oversee enterprise-wide functions of Finance, Procurement, IT and Human Resources. Many other examples further demonstrate efforts made in this regard, and DBHDS Senior Leadership remains committed to continuous improvement for oversight of agency and system-wide functions and activities across the Commonwealth.

We appreciate your team's efforts, constructive feedback, and acknowledgement of resource limitations and other challenges facing DBHDS. The recommendations provided by APA will help focus our efforts and support our desire to properly resource and oversee several functional areas across the Commonwealth. Please contact Alvie Edwards, Director of Internal Audit, if you have any questions regarding our corrective action plan.

Sincerely,

Alison G. Land, FACHE
Commissioner

COMMONWEALTH of VIRGINIA
Department of Health
P O BOX 2448
RICHMOND, VA 23218
TDD 1-800-828-1120

December 20, 2019

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

Dear Ms. Mavredes:

We have reviewed your report on our audit for the year ended June 30, 2019. We concur with the findings and our corrective action plan will be provided in accordance with the Department of Account guidelines.

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

Sincerely,

M. Norman Oliver MD

M. Norman Oliver, MD, MA
State Health Commissioner

VDH VIRGINIA DEPARTMENT OF HEALTH
Protecting You and Your Environment
www.vdh.state.va.us

KAREN KIMSEY
DIRECTOR

COMMONWEALTH of VIRGINIA

Department of Medical Assistance Services

804-786-7933
www.dmas.virginia.gov

January 8, 2020

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

Dear Ms. Mavredes:

We have reviewed the draft Management Report for the Department of Medical Assistance Services (DMAS) that will be included in the report for the Audit of the Agencies of the Secretary of Health and Human Resources for the Fiscal Year Ending June 30, 2019. We concur with the audit findings assigned to DMAS. We will send a response to the Department of Accounts, within the required thirty days after the report is issued. The response will include the workplan for corrective actions to be taken to address the audit findings.

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

Sincerely,

Karen Kimsey

Karen Kimsey

600 EAST BROAD STREET • SUITE 1300 • RICHMOND, VIRGINIA 23219 • 800-343-0634 (TDD)

COMMONWEALTH of VIRGINIA

DEPARTMENT OF SOCIAL SERVICES

Office of the Commissioner

S. Duke Storen
COMMISSIONER

January 21, 2020

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

Dear Ms. Mavredes:

The Virginia Department of Social Services concurs with the audit findings included in the 2019 review by the Auditor of Pulic Accounts.

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

Sincerely,

S. Duke Storen

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

AGENCIES OF THE SECRETARY OF HEATH AND HUMAN RESOURCES

As of June 30, 2019

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

Department of Behavioral Health and Developmental Services

S. Hughes Melton, M.D., MBA, FAAFP, FABAM – Commissioner

Department of Health

M. Norman Oliver, M.D., MA – Commissioner

Department of Medical Assistance Services

Jennifer S. Lee, M.D. – Director

Department of Social Services

S. Duke Storen – Commissioner