DEPARTMENT OF BEHAVIORAL HEALTH AND DEVELOPMENTAL SERVICES

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2024

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

AUDIT SUMMARY

Our audit of the Department of Behavioral Health and Developmental Services (DBHDS) for the year ended June 30, 2024, found:

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

- twelve matters involving internal control and its operation necessary to bring to management's attention, eleven of which also represent instances of noncompliance with applicable laws and regulations or other matters that are required to be reported; and

- adequate corrective action with respect to four prior audit findings and recommendations identified as complete in the Findings Summary included in the Appendix.

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

Our report includes two risk alerts that require the action and cooperation of DBHDS' management and the Virginia Information Technologies Agency (VITA) regarding risks related to unpatched software and access to centralized audit log information.

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

-TABLE OF CONTENTS-

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

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

DBHDS continues to make limited progress to document baseline configurations for its sensitive systems' hardware and software requirements. Additionally, DBHDS did not perform annual reviews for the four baseline configurations it completed in the prior year. Baseline security configurations are essential controls in information technology environments to ensure that systems have appropriate configurations and serve as a basis for implementing or changing existing information systems.

Since the prior year audit, DBHDS reduced its information system environment from 90 to 52 sensitive systems and applications across the Central Office and 12 facilities, with some containing Health Insurance Portability and Accountability Act (HIPAA) data, social security numbers, and Personal Health Information data. Additionally, DBHDS developed a baseline configuration for one of its 52 (2%) sensitive systems during the 2024 fiscal year, totaling five baseline configurations (6%) for its 52 sensitive systems in the last two years.

The Commonwealth's Information Security Standard, SEC530 (Security Standard), requires DBHDS to perform the following:

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

The absence of baseline configurations increases the risk that these systems will not meet the minimum-security requirements to protect data from malicious access attempts. If a data breach occurs to a system containing HIPAA data, DBHDS can incur large penalties, up to $1.5 million.

The limited progress made in the last year is partially due to DBHDS' ongoing efforts to reduce its inventory of sensitive systems to a manageable state. Additionally, DBHDS' changes to the staff allocated to complete its corrective actions have caused additional delays in completing the baseline configurations. DBHDS should assign the necessary resources to continue its efforts to complete baseline configurations for the remaining existing systems as well as new systems implemented in the future. DBHDS should also establish a process to maintain security baseline configurations for its sensitive systems to meet the requirements of the Security Standard and protect the confidentiality, integrity, and availability of the agency's sensitive data.

Continue to Improve Database Security

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

DBHDS continues not to secure the database server that supports its financial system in accordance with its internal policies, the Security Standard, and industry best practices, such as the Center for Internet Security Benchmarks. We communicated three control weaknesses related to baseline configuration and lack of policies and procedures for review and restore processes to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

The Security Standard requires DBHDS to implement certain security controls to safeguard systems that contain or process sensitive data. By not meeting the minimum requirements in the Security Standard and industry best practices, DBHDS cannot ensure the confidentiality, integrity, and availability of data within its system.

DBHDS works with an external vendor to manage its financial system. While the external vendor provided verbal justifications in prior years for deviating from certain controls required by the Security Standard or recommended by industry best practices, DBHDS did not verify, approve, and document the deviations and justifications in its baseline configuration, nor did DBHDS enforce the baseline's expected configuration. DBHDS discovered during fiscal year 2024 that the database was not capable of meeting the requirements of the Security Standard and is in the process of developing a new corrective action plan. Additionally, DBHDS' lack of management oversight led to the weaknesses outlined in the FOIAE communication.

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

should also include the requirements in its policy and procedure for its review and restore processes. These actions will help to protect the confidentiality, integrity, and availability of DBHDS's mission critical and sensitive data.

Improve IT Contingency Management Program

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2017

DBHDS has made limited progress to complete updated Continuity of Operations Plans (COOP) and IT Disaster Recovery Plans (DRP) for its 12 facilities and Central Office. As of the end of fiscal year 2024, DBHDS has completed nine COOPs and DRPs (69%) out of 13 expected, but the completed documents do not meet all requirements as prescribed in the Security Standard. Additionally, the Central Office and facilities do not perform annual reviews and tests of the completed COOPs or DRPs to verify their adequacy and effectiveness.

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

By not having current and complete COOPs and DRPs for all 12 facilities and the Central Office, DBHDS increases the risk of mission critical systems being unavailable to support patient services. In addition, by not performing annual tests against the COOPs and DRPs, DBHDS is unable to identify weaknesses in the plans and may unnecessarily delay the availability of sensitive systems in the event of a disaster or outage.

While each DBHDS facility and the Central Office are responsible for creating their individual COOP and DRP, the Central Office's Information Technology and Emergency Planning departments are responsible for ensuring all facilities complete the COOPs and DRPs as required by the Security Standard. The lack of communication and coordination between the Central Office's Information Technology and Emergency Planning departments and individual facilities, as well as DBHDS' misinterpretation of testing requirements, have caused delays in completing the COOPs and DRPs accurately and fully. Additionally, DBHDS' changes to the staff allocated to complete its corrective actions have caused additional delays in resolving this finding.

DBHDS should ensure there is adequate coordination among departments and facilities to update the contingency management program for the Central Office and facilities to meet the minimum requirements in the Security Standard. DBHDS should update the COOPs and DRPs ensuring they meet all requirements in the Security Standard and are consistent with the agency's IT risk management documentation and across the facilities and Central Office. Once DBHDS completes the contingency documents, it should conduct tests on at least an annual basis to ensure the Central Office and facilities can restore mission critical and sensitive systems in a timely manner in the event of an outage or disaster.

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

DBHDS has made limited progress in conducting risk assessments over its sensitive systems in accordance with the Security Standard and the Commonwealth's Information Technology Risk Management Standard, SEC520 (Risk Management Standard). As of the end of fiscal year 2024, DBHDS has completed three risk assessments (5%) and drafted an additional seven (13%) out of its 52 sensitive systems. However, DBHDS has not completed a risk treatment plan for any of the risk assessments drafted during fiscal year 2024.

The Security Standard requires DBHDS to conduct and document a risk assessment of IT systems as needed, but not less than once every three years, and conduct and document an annual self-assessment to determine the continued validity of the risk assessment. Additionally, the Risk Management Standard requires DBHDS to submit a risk treatment plan for each risk with a residual risk greater than low to the Commonwealth's Chief Information Security Officer (CISO) within 30 days of the final risk assessment report.

Without conducting risk assessments and risk treatment plans for all systems, DBHDS increases the risk that it will not detect and mitigate existing weaknesses in the IT environment. By not detecting the weaknesses, it increases the risk of a malicious user compromising sensitive data and impacting the system's availability. The limited progress made in the last year is partially due to DBHDS' ongoing efforts to reduce its inventory of sensitive systems to a manageable state. Additionally, DBHDS' changes to the staff allocated to complete its corrective actions have caused additional delays in completing the risk assessments and risk treatment plans.

DBHDS should complete a risk assessment for its remaining sensitive systems. DBHDS should also complete a risk treatment plan for those risks identified with a residual risk greater than low that details the necessary information. Additionally, DBHDS should conduct an annual self-assessment for its completed risk assessments to determine the continued validity of the risk assessment. These actions will help DBHDS identify potential risks and implement adequate controls to mitigate risk to its individual systems, IT environments, and business operations.

Continue to Improve Off-Boarding Procedures
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2014

DBHDS is not properly off-boarding employees, retaining appropriate documentation to support the completion of off-boarding procedures, and removing system access for employees timely. Our review of terminated employees included reviewing off-boarding processes at four different facilities and reviewing system access removals for the entire agency. When reviewing off-boarding processes, we identified that two of the four facilities tested were not consistently completing an off-boarding

checklist for terminated employees or entering employee termination dates in the Commonwealth's accounting and financial reporting system timely. During our review, we specifically identified the following deficiencies:

- For 14 of 20 (70%) employees tested at two DBHDS facilities under review, the facilities did not complete an off-boarding checklist.

- For three of 20 (15%) terminated employees tested at two DBHDS facilities, the facilities could not provide a resignation letter or other supporting documentation to agree to the date of termination in the system.

- For 11 of 20 (55%) terminated employees tested at two DBHDS facilities, the facilities could not provide supporting documentation showing the employees returned state property by their termination date.

- For eight of 20 (40%) terminated employees tested at two DBHDS facilities, the facilities did not remove building or system access within 24 hours of the employee's separation.

- For two of four (50%) terminated employees tested at four DBHDS facilities, DBHDS did not remove access to the Commonwealth's retirement benefits system within 24 hours of the employee's separation.

- For 12 of 21 (57%) terminated employees tested at DBHDS, DBHDS did not remove access to the internal patient revenue system within 24 hours of the employee's separation.

- For 14 of 27 (52%) terminated employees tested at DBHDS, DBHDS did not enter the employee's termination date timely which led to the untimely removal of the employee's access to the Commonwealth's accounting and financial reporting system.

DBHDS's Central Office has provided facilities with off-boarding guidance and a termination checklist, which the facilities were to incorporate into their existing procedures. The Security Standard states an organization must disable accounts within 24 hours when the accounts have expired, are no longer associated with a user or individual, are in violation of organizational policy, or have been inactive for 90 days.

DBHDS experienced a high volume of turnover during the period under review. The volume of turnover was a contributing factor to these issues, as well as other factors such as a lack of communication, lack of oversight, competing prioritized tasks, job abandonment, and insufficient implementation of policies and procedures. Without sufficient and documented internal controls over terminated employees that ensure the return of Commonwealth property and removal of all access privileges, DBHDS is increasing the risk that terminated employees may retain physical access to Commonwealth property and unauthorized access to internal systems, which may include sensitive

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

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

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

DBHDS has made progress to retain its resources to manage its information security program and IT projects. As of September 2024, DBHDS retained its six Information Security Officers (ISOs) and two contractors hired for the past two years. Additionally, DBHDS has reduced its number of sensitive systems and applications from 90 in the prior year to 52 between the Central Office and its facilities, which assists DBHDS in ensuring compliance with the agency's enterprise security program and the Security Standard.

While DBHDS has filled all IT positions, DBHDS delegated the staff to other agency priorities in prior years. Prior to 2022, DBHDS delegated the ISOs to work on remediation efforts, such as completing baseline configurations and risk assessments for its sensitive systems. In 2022, DBHDS reallocated duties from the ISOs to the contractors to continue remediation efforts and then reallocated the duties back to the ISOs to complete corrective actions in fiscal year 2024. Additionally, DBHDS has continued to revise its intended completion dates for reported corrective actions, causing the extension of some corrective actions by as much as three years. These actions have limited DBHDS' ability to make significant progress in improving its information security program and remediate prior years' management recommendations, one of which has been ongoing for nine years.

Per the Security Standard, agency heads are responsible for ensuring the agency maintains, documents, and effectively communicates a sufficient information security program to protect the agency's IT systems. Without completing corrective actions, DBHDS risks gaps in key security control areas, making it more susceptible to attacks and breaches. Additionally, due to the use of health data in its sensitive systems, DBHDS risks a breach of HIPAA data, which may lead to large penalties, as much as $1.5 million.

DBHDS should continue its efforts to reduce its sensitive system inventory. DBHDS should review its corrective action plans to establish realistic timelines and completion dates. DBHDS should also establish clear milestones based on priority for corrective action plans to ensure that it efficiently

allocates its resources. Additionally, DBHDS should dedicate the necessary resources across the agency to meet the completion dates within its corrective action plans.

Continue to Implement Compliant Application Access Management Procedures
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2018

DBHDS continues to focus on implementing compliant access management procedures at the facility level that meet the baseline standard defined by the Security Standard. In fiscal year 2024, DBHDS completed a two-year project working with the facilities to provide proper training on compliant application procedures at the facility level. However, due to the number of applications and competing priorities within the Information Security Office, DBHDS has yet to confirm that all facilities have implemented appropriate access management procedures.

DBHDS has been working to reduce and standardize applications across the agency to aid in having baseline policies and procedures established across DBHDS and the facilities. DBHDS plans to hire a contractor to ensure that all applications are single sign-on compliant and automatically remove users from systems when off-boarded.

The Security Standard, 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. In addition, the Security Standard addresses requirements over account management practices for requesting, granting, administering, and terminating accounts. Not having adequate access control policies and procedures increases the risk that individuals will have inappropriate access and can potentially process unauthorized transactions.

DBHDS should continue to reduce and standardize applications across the agency as necessary and continue to work with facilities to set reasonable deadlines for implementing access management procedures. DBHDS should ensure that facilities properly implement adequate application access management procedures that align with DBHDS' baseline procedures and the Security Standard.

Improve Security Awareness Training Program
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2023

DBHDS has made progress administering its security awareness training program in accordance with its IT Security Awareness and Training Policy (Security Awareness Policy), the Security Standard, and the Commonwealth's Security Awareness Training Standard, SEC527 (Security Awareness Training Standard). DBHDS resolved one of the three weaknesses from the prior year audit by monitoring and enforcing its annual security awareness training for its employees and contractors. However, DBHDS continues to have the following two weaknesses in its security awareness training program:

- DBHDS does not provide role-based training to all users with designated security roles, such as System Owners, Data Owners, System Administrators, Agency Head, security personnel, etc. While DBHDS developed some role-based training modules during the 2024 calendar year, the agency has not finalized and tested the role-based modules for the applicable personnel due to other priorities and resource constraints, causing DBHDS to delay its implementation of role-based training. DBHDS' Security Awareness Policy, which is based on the Security Standard, requires that the agency provide role-based security training commensurate with the user's level of expertise. The lack of adequate role-based training increases the risk that users will be unaware or unequipped to perform their assigned security-related functions, resulting in an increased data security risk.

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

While DBHDS did not have the resources necessary to develop specific role-based modules prior to the 2023 training campaign, as of November 2024, DBHDS developed and tested role-based modules that the agency expects to assign to employees in 2025. Additionally, DBHDS' CISO is responsible for reviewing the agency's policies and procedures, but due to other competing priorities, the CISO was unable to review and update the Security Awareness Policy.

DBHDS should dedicate the necessary resources to conduct annual reviews and revise the Security Awareness Policy, as necessary, to ensure its policy requirements align with those outlined in the Security Standard and Security Awareness Training Standard. Additionally, DBHDS should finalize and administer role-based training to users with designated security roles, which will help the agency be aware of malicious attempts to compromise the confidentiality, integrity, and availability of sensitive information.

Improve Oversight of Third-Party Service Providers

Type: Internal Control and Compliance
Severity: Significant Deficiency

DBHDS does not have sufficient internal controls over System and Organization Controls (SOC) reports for third-party service providers. DBHDS utilizes a grants management system hosted by a service provider for tracking prime awards and subawards that it disburses to Community Service Boards. SOC reports, specifically SOC 2, Type II reports, provide an independent description and evaluation of the operating effectiveness of service providers' internal controls and are a key internal control in gaining an understanding of a service provider's internal control environment and maintaining oversight over

outsourced operations. DBHDS did not obtain, review, or document the review of the grants management system SOC report to identify deficiencies or determine whether the report provided adequate coverage over operations during state fiscal year 2024.

The Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic 10305 requires agencies to have adequate interaction with service providers to appropriately understand the service provider's internal control environment. Agencies must also maintain oversight over service providers to gain assurance over outsourced operations. Additionally, the Security Standard states that agency heads remain accountable for maintaining compliance with the Security Standard for IT equipment, systems, and services procured from service providers, and must enforce the compliance requirements through documented agreements and oversight with service providers for the services they provide.

Without obtaining and reviewing SOC reports over all relevant service providers, DBHDS is unable to ensure its complementary user entity controls are sufficient to support their reliance on the service providers' control design, implementation, and operating effectiveness. Additionally, DBHDS is unable to address any internal control deficiencies and/or expectations identified in the SOC report. DBHDS is increasing the risk that it will not detect a weakness in a service provider's environment by not obtaining the necessary SOC reports or properly documenting its review of the report.

DBHDS did not obtain a SOC report for the grants management system due to management oversight. DBHDS failed to obtain and review the SOC report to ensure that security measures in place were reasonable for how DBHDS utilizes the system. DBHDS should obtain, review, and document the review of SOC 2, Type II reports for its grants management system. In addition, DBHDS should evaluate all other service providers it uses to determine if it should obtain and review SOC 2, Type II reports for any other service provider. DBHDS should ensure these reviews comply with the requirements outlined in the CAPP Manual and the Security Standard. DBHDS should communicate this requirement to all individuals responsible for overseeing service provider operations to ensure compliance with Commonwealth regulations.

Continue to Improve Controls over the Calculation of Contractual Commitments

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

DBHDS should continue to improve controls over the calculation of contractual commitments which they report to Accounts for inclusion in the Commonwealth's Annual Comprehensive Financial Report (ACFR). DBHDS did not compile and calculate its contractual commitments accurately for fiscal year 2024. DBHDS' process for calculating the commitments disclosure did not include all the necessary contracts that were a commitment as of year-end, it improperly included additional contracts that it should have excluded, and there were errors in the data used for the calculation. These weaknesses resulted in an overstatement of contractual commitments of approximately $12.1 million.

DBHDS experienced turnover in the positions that are responsible for contractual commitment calculations including positions within Procurement, and Architectural and Engineering which

contributed to the identified weaknesses. In addition to the turnover, DBHDS does not have sufficiently detailed procedures for how DBHDS should compile and calculate the commitments disclosure. Since the prior year, DBHDS has developed policies and procedures over the calculation of year-end commitments. However, the policies and procedures do not provide enough detail regarding all required steps to allow staff to perform the calculation accurately. While these weaknesses did not have a material impact for fiscal year 2024, if left unaddressed, there is an increased risk that DBHDS will report inaccurate commitment amounts which could be misleading to users of the ACFR. Accounts Comptroller's Directive No. 1-24 establishes compliance guidelines and addresses financial reporting requirements for state agencies to provide information to Accounts for the preparation of the ACFR as required by the Code of Virginia. Accounts requires state agencies to submit information as prescribed in the Comptroller's Directives and individuals preparing and reviewing the submissions must certify the accuracy of the information provided to Accounts.

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

Improve Change Management Process for Information Technology Environment

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

DBHDS has made significant progress to improve and consistently follow its formal change control and configuration management process. While DBHDS has remediated two of the three prior year's weaknesses, DBHDS continues to not annually review and revise, as needed, its IT Configuration Management Policy, which it last reviewed in December 2021.

The Security Standard requires DBHDS to review and update the configuration management policy on an annual basis or more frequently if required to address an environmental change. By not performing annual policy reviews, DBHDS cannot ensure it properly communicates, implements, and enforces its new security control and process requirements, which increases the risk of implementing unauthorized changes in the IT environment.

DBHDS' CISO is responsible for reviewing the agency's policies and procedures, but due to other competing priorities, the CISO was unable to review and update the IT Configuration Management Policy. DBHDS should annually review its IT Configuration Management Policy to ensure it consistently documents DBHDS' expectations for its change management process and continues to align with the Security Standard. Maintaining and effective change management process will help to protect the confidentiality, integrity, and availability of sensitive and mission essential data.

Ensure Compliance with the Conflict of Interests Act

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

In fiscal year 2021, DBHDS did not properly identify and track individuals in a position of trust to ensure compliance with the Conflict of Interests Act (COIA) requirements. In addition, DBHDS did not ensure the required employees completed the mandatory training. DBHDS has since provided policies and procedures regarding COIA compliance requirements to all DBHDS facilities. DBHDS Central Office Human Resources is now in the process of monitoring all DBHDS facilities to ensure they meet all necessary training requirements within the two-year required timeframe; however, corrective action remains ongoing and DBHDS continues to improve its processes to ensure compliance with all COIA requirements. Due to ongoing corrective action during the period under audit, we did not perform testing of compliance with COIA requirements during the current audit.

Per § 2.2-3114 of the Code of Virginia, persons occupying positions of trust within state government or non-salaried citizen members of policy and supervisory boards shall file a disclosure statement with the Commonwealth's Ethics Advisory Council, as a condition to assuming office or employment, and thereafter shall file such a statement annually on or before February 1. Section 2.2-3130 of the Code of Virginia requires that each employee within a position of trust complete COIA training within two months of their hire date and at least once every two years after the initial training.

Without appropriately identifying employees in positions of trust and ensuring completion of required training, DBHDS could be susceptible to actual or perceived conflicts of interest and may limit its ability to hold its employees accountable for not knowing how to recognize and resolve a conflict of interest. Employees and board members could be subject to penalties for inadequate disclosure on their filings, as outlined within § 2.2-3120 through § 2.2-3127 of the Code of Virginia.

DBHDS should continue to monitor all DBHDS facilities to ensure that employees within positions of trust file the appropriate disclosures upon hire or promotion, and subsequently at each annual filing period. In addition, DBHDS should continue to monitor employees to ensure they complete the required COIA training timely.

RISK ALERTS

During our audit, we encountered issues that are beyond the corrective action of DBHDS management alone and require the action and cooperation of management and VITA. The following issues represent such a risk to DBHDS and the Commonwealth.

Unpatched Software
First Reported: Fiscal Year 2021

VITA contracts with various providers to create the Commonwealth's Information Technology Infrastructure Services Program (ITISP) to provide agencies with installation, maintenance, operation, and support of IT infrastructure components, such as servers, routers, firewalls, and virtual private networks. DBHDS continues to rely on contractors procured by VITA for the installation of security patches in systems that support DBHDS' operations. Additionally, DBHDS relies on VITA as the contract administrator to maintain oversight and enforce the contract agreements with the ITISP contractors. As of July 2024, the ITISP contactors had not applied a significant number of security patches that are critical and highly important to DBHDS' IT infrastructure components, all of which are past the 30-day update window allowed by the Security Standard.

The Security Standard requires the installation of security-relevant software and firmware updates within 30 days of release or within a timeframe approved by VITA's Commonwealth Security and Risk Management division. The Security Standard does allow for varying time periods depending on factors such as the criticality of the update, but generally the ITISP uses a 30-day window from the date of release as its standard for determining timely implementation of security patches. Missing system security updates increases the risk of successful cyberattack, exploit, and data breach by malicious parties.

While VITA is responsible for enforcing the service level agreement, it has not been able to compel the current ITISP contractors to install certain security patches to DBHDS' IT infrastructure to remediate vulnerabilities in a timely manner or take actions to obtain these required services from another source. DBHDS is working with VITA and the ITISP contractors to ensure that the ITISP contractors install all critical and highly important security patches on all servers. Our separate audit of VITA's contract management will also continue to report this issue.

Access to Centralized Audit Log Information
First Reported: Fiscal Year 2021

DBHDS relies on the Commonwealth's ITISP to install, maintain, operate, and support IT infrastructure components, such as servers, routers, firewalls, and virtual private networks. As part of these services, DBHDS relies on contractors procured by VITA to provide DBHDS access to a centralized monitoring tool, known as the Managed, Detection, Response (MDR) Dashboard, that collects audit log information about activities in DBHDS' IT environment so that DBHDS can review logged activity. Additionally, DBHDS relies on VITA to maintain oversight and enforce the service level agreements and deliverables with the ITISP contractors.

While VITA did not originally enforce the deliverable requirement when ratifying the ITISP contracts in 2018, VITA tried to compel the ITISP contractor to grant agencies, such as DBHDS, access to the monitoring tool and audit log information for the last five years. The MDR Dashboard went live in October 2023 but did not include all audit log information to allow agencies to adequately monitor their IT environments. Additionally, VITA implemented a separate security and event management (SIEM) tool at the end of October 2023 to expand agencies' capabilities to monitor audit log information. As of October 2024, VITA and the ITISP supplier determined the MDR Dashboard will be replaced by the VITA-managed SIEM tool as the permanent audit log monitoring tool. However, while the VITA-managed SIEM tool is in production, it also does not include all audit log information in a usable format to allow agencies to adequately monitor their IT environments.

The Security Standard requires a review and analysis of audit records at least every 30 days for indications of inappropriate or unusual activity and assessment of the potential impact of the inappropriate or unusual activity. Using a SIEM tool without all necessary audit log information reduces organizational security posture by not being able to react to and investigate suspicious system activity in a timely manner. DBHDS is working with VITA to import audit log information to the SIEM tool and provide feedback on its uses to ensure DBHDS can review the activities occurring in its IT environment in accordance with the Security Standard. Our separate audit of VITA's contract management will also continue to report this issue.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 13, 2024

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Janet Kelly
Secretary of Health and Human Resources

Nelson Smith
Commissioner, Department of Behavioral Health and Developmental Services

We have audited the financial records and operations of **Department of Behavioral Health and Developmental Services** (DBHDS) for the year ended June 30, 2024. We conducted this audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, in support of the Commonwealth's Annual Comprehensive Financial Report audit. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Objectives

Our audit's primary objective was to evaluate the accuracy of DBHDS' financial transactions as reported in the Annual Comprehensive Financial Report for the Commonwealth of Virginia for the year ended June 30, 2024. In support of this objective, we evaluated the accuracy of recorded financial transactions in the Commonwealth's accounting and financial reporting system, DBHDS' financial system, and supplemental information and attachments submitted to the Department of Accounts; reviewed the adequacy of DBHDS' internal control; tested for compliance with applicable laws, regulations, contracts, and grant agreements; and reviewed corrective actions with respect to audit findings and recommendations from prior year reports.

Audit Scope and Methodology

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

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

Commonwealth's retirement benefit system
Information system security (including access controls)
Institutional revenues
Licensing behavioral health providers
Operational expenses, including payroll expenses

We performed audit tests to determine whether DBHDS' 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 DBHDS' operations. We performed analytical procedures, including budgetary and trend analyses, and tested details of transactions to achieve our audit objectives.

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

Our consideration of internal control over financial reporting (internal control) was for the limited purpose described in the section "Audit Objectives" and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control, which are described in the section titled "Internal Control and Compliance Findings and Recommendations" that we consider to be significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a

combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. 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.

Conclusions

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

We noted certain matters involving internal control and its operation and compliance with applicable laws, regulations, contracts, and grant agreements that require management's attention and corrective action. These matters are described in the section titled "Internal Control and Compliance Findings and Recommendations."

DBHDS has taken adequate corrective action with respect to four prior audit findings identified as complete in the Findings Summary included in the Appendix.

Since the findings noted above include those that have been identified as 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," which is included in the Commonwealth of Virginia's Single Audit Report for the year ended June 30, 2024. The Single Audit report will be available at www.apa.virginia.gov in February 2025.

Exit Conference and Report Distribution

We discussed this report with management at an exit conference held on January 9, 2025. Government Auditing Standards require the auditor to perform limited procedures on DBHDS' response to the findings identified in our audit, which is included in the accompanying section titled "Agency Response." DBHDS' response was not subjected to the other auditing procedures applied in the audit and, accordingly, we express no opinion on the response.

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

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

JDE/clj

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	First Reported for Fiscal Year
Continue to Improve Controls over the Retirement Benefits System Reconciliation	Complete	2014
Continue to Improve Controls over Payroll Reconciliations	Complete	2020
Conduct Information Technology Security Audits Over Sensitive Systems	Complete	2022
Improve Vulnerability Management Process	Complete	2022
Improve Controls over the Payroll Certification Process	Complete	2023
Develop Baseline Configurations for Information Systems	Ongoing	2015
Continue to Improve Database Security	Ongoing	2021
Improve IT Contingency Management Program	Ongoing	2017
Continue to Improve Risk Assessment Process	Ongoing	2021
Continue to Improve Off-Boarding Procedures	Ongoing	2014
Continue Dedicating Resources to Support Information Security Program	Ongoing	2019
Continue to Implement Compliant Application Access Management Procedures	Ongoing	2018
Improve Security Awareness Training Program	Ongoing	2023
Improve Oversight of Third-Party Service Providers	Ongoing	2024
Continue to Improve Controls over the Calculation of Contractual Commitments	Ongoing	2021
Improve Change Management Process for Information Technology Environment	Ongoing	2023
Ensure Compliance with the Conflict of Interests Act	Ongoing	2021
Complete FFATA Reporting for First Tier SABG Subawards	Ongoing**	2022

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

** This audit finding originated from the fiscal year 2022 audit of the Substance Abuse Block Grant federal grant program. This federal grant program is not in cycle for the Commonwealth's 2024 Single Audit, and as such, we limited our audit procedures to confirming the accuracy of the corrective action status in the Commonwealth's Summary Schedule of Prior Audit Findings. Per our inquiry with DBHDS, we determined that corrective action was ongoing as of June 30, 2024.

COMMONWEALTH of VIRGINIA

NELSON SMITH
COMMISSIONER

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

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

January 17, 2025

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

Dear Ms. Henshaw:

We have reviewed your report on our audit for the year ended June 30, 2024. We concur with the findings and our corrective action plans have been provided separately.

The Virginia Department of Behavioral Health and Developmental Services (DBHDS) has made significant progress to close several findings from prior year audit, and we appreciate that this report reflects the progress made to date on those corrective actions. Based on our progress demonstrated during this audit cycle, we are committed and will work to resolve and close several of the findings identified during this audit cycle. We greatly appreciate the audit team's interest and effort to evaluate risks we face due to decentralization, and the acknowledgement of ongoing efforts to identify resources and other interventions to mitigate the risks associated with these ongoing challenges. Despite continuing to face unprecedented challenges in the behavioral health and developmental disability community this fiscal year, we are proud of our staff for their incredible efforts to face those challenges while remaining committed to enhancing our operations and system of care.

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

Sincerely,

Nelson Smith
Commissioner