DEPARTMENT OF HEALTH

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 Health (Health), including the federal grant programs: Activities to Support State, Tribal, Local and Territorial (STLT) Health Department Response to Public Health or Healthcare Crises; Coronavirus State and Local Fiscal Recovery Funds; Drinking Water State Revolving Fund; and Epidemiology and Laboratory Capacity for Infectious Diseases, for the fiscal year ended June 30, 2024, found:

- proper recording and reporting of all transactions, in all material respects, in the Commonwealth's accounting and financial reporting system, Health's accounting and financial reporting system, and supplemental information and attachments submitted to the Department of Accounts (Accounts), after adjustment for the misstatement noted in the finding titled "Strengthen Controls over Financial Reporting;"
- two matters involving internal control and its operation necessary to bring to management's attention, one of which is considered a significant deficiency and one that is considered a material weakness;
- nine matters involving internal control and its operation necessary to bring to management's attention that 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 two 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 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.

Health is one of several entities cited in a risk alert in Accounts fiscal year 2024 audit report. The "Financial Reporting" risk alert identifies the increased risk that the Commonwealth may not meet the deadline for the Annual Comprehensive Financial Report, which could jeopardize the Commonwealth's bond rating, because multiple entities have increasingly submitted inaccurate and late financial information to Accounts over the past several fiscal years. As an entity that is contributing to this increased risk for the Commonwealth, Health's corrective action to correct the issues in the finding titled "Strengthen Controls over Financial Reporting" is essential to reducing the risk to the Commonwealth.

Additionally, Health's report includes one risk alert that requires the action and cooperation of Health's management and the Virginia Information Technologies Agency (VITA) regarding risks related to unpatched software.

In fiscal year 2023, we included the results of our audit over Health 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

Strengthen Controls over Financial Reporting
Type: Internal Control
Severity: Material Weakness
First Reported: Fiscal Year 2021

The Department of Health (Health) does not have adequate controls over financial reporting information submitted to the Department of Accounts (Accounts). Health's Office of Financial Management (OFM) is responsible for submitting information to Accounts, including multiple attachments used in the preparation of the Commonwealth's financial statements. There were several instances where information Health submitted to Accounts was late or contained errors requiring resubmission as follows:

- OFM reports information on accounts receivable to Accounts on the Receivables as of June 30 Attachment (Receivables Attachment). The initial Receivables Attachment OFM submitted included $4.5 million in formula rebates for the Women, Infants and Children (WIC) program misclassified as a revenue receivable. The second Receivables Attachment OFM submitted erroneously included a $105 million receivable for the Coronavirus State and Local Fiscal Recovery Fund. To correct the errors, OFM submitted two subsequent revisions to Accounts.

- OFM reports information on federal expenditures to Accounts on the Federal Schedules Attachment (Federal Attachment), which includes the Schedule of Expenditures of Federal Awards (SEFA). The initial Federal Attachment SEFA submission overstated federal expenditures by a total of $88.1 million, while the second Federal Attachment SEFA submission understated federal expenditures by a total of $10.3 million. The Federal Attachment also includes a reconciliation between information reported on the attachment and the Commonwealth's accounting and financial reporting system. On the initial Federal Attachment reconciliation submission, the reconciling items did not agree to supporting documentation and Health misstated the reconciling items by $79.1 million. In the second submission, Health overstated one reconciling item by $80.4 million and another by $89.3 million due to OFM modifying amounts reported initially, which were correct, and not correctly adjusting the original misstatement. To correct the errors, OFM submitted a third revision to Accounts, which contained a reconciliation misclassification of $107.6 million. While this reconciliation misstatement did not require adjustment, as it did not cause a misstatement on the SEFA, it continued to indicate a weakness in internal controls.

- OFM improved the timeliness of required attachment and supplemental item submissions to Accounts; however, the need for resubmissions for errors identified by Health delayed the reporting of auditable financial information. These delays included the Receivables Attachment, for which the first auditable version was 56 days late, and the Federal Attachment, which was 61 days late. In addition, OFM took three months to complete subsequent adjusted submissions of the Federal Attachment.

Health's financial activity is material to the Commonwealth's financial statements, so it is essential for Health to have strong financial reporting practices. As best practices, OFM should submit accurate financial reporting information to Accounts by the associated due dates and communicate any expected delays to Accounts as soon as they are known.

Several factors contributed to these financial reporting issues. OFM has experienced a significant amount of turnover in key positions during the last three fiscal years, including multiple at the end of fiscal year 2024. Health shifted existing resources after fiscal year end, during the attachment compilation process, for positions that were historically responsible for completing and submitting attachments to Accounts. However, there were not adequate policies and procedures for staff to use as a resource. In addition, errors in a report obtained from Health's accounting and financial reporting system, and the lack of sufficient controls to detect and prevent errors, resulted in the misstatements mentioned above on the Federal Attachment. The lack of adequate policies and procedures that establish sufficient controls to detect and prevent errors increases the risk that information reported to Accounts to compile the Commonwealth's financial statements could be materially misstated.

In recent months, Health's management initiated a reorganization that aims to address leadership and staffing needs for the OFM division. Health's management should continue to work with OFM to fill vacant positions and to ensure a more stable and adequate staffing level. As part of its corrective actions, OFM should ensure it has adequate written policies and procedures in place over key processes, as well as identify opportunities for cross-training. These actions will ensure that adequate resources are in place to mitigate the effects of significant turnover in the future, and that OFM implements controls to detect and prevent errors. Lastly, OFM should prioritize training new employees in key positions to improve the quality of financial information reported to Accounts.

Continue Strengthening the System Access Removal Process

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

Health did not remove terminated employees' access to critical information systems in a timely manner following the employees' separation from the agency. During our review, we found that Health did not remove system access timely for 246 of 492 (50%) terminated users of Health's patient management system. These accounts were removed two to 3,404 days after the employees' termination dates.

The Commonwealth's Information Security Standard, SEC530 (Security Standard), states an organization must disable information system access within 24 hours of employee separation and terminate any authenticators or credentials associated with the individual. Untimely termination of system access increases the risk of terminated employees retaining unauthorized access to state systems and sensitive information and increases the risk of inappropriate transactions and exposure of sensitive data.

During fiscal year 2024, Health performed a review of roles in the patient management system, which resulted in Health removing a significant number of outdated users. Health's Office of Information Management (OIM) also implemented a compensating control that restricts user access to the patient management system once Health terminates the user's email. This modification should reduce risks associated with the late removal of system access to the patient management system; however, the automated control was not in effect for all of fiscal year 2024 and therefore, we will review this control during next year's audit.

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

Review Subrecipient Audit Reports
Type: Internal Control and Compliance
Severity: Significant Deficiency

Health does not monitor subrecipients in accordance with federal regulations for the Epidemiology and Laboratory Capacity for Infectious Diseases (ELC) and Activities to Support State, Tribal, Local and Territorial (STLT) Health Department Response to Public Health or Healthcare Crises federal grant programs. During our audit, we found that Health's Office of Epidemiology (Epidemiology) and the Office of Health Equity (OHE) did not obtain and review a Single Audit or program-specific audit report for subrecipients who received $750,000 or more in subawards from ELC and STLT funds.

During fiscal year 2024, Health disbursed approximately $11 million in ELC funds and $5.8 million in STLT funds to subrecipients. According to Title 2 U.S. Code of Federal Regulations (CFR) § 200.332(f), all pass-through entities must verify their subrecipients are audited if it is expected that the subrecipient's federal awards expended during the respective fiscal year will equal or exceed $750,000. Additionally, in the case of any findings, 2 CFR § 200.332(d)(3) requires pass-through entities to issue a management decision within six months of acceptance of the audit report by the Federal Audit Clearinghouse (Clearinghouse).

Due to significant turnover in contract administrators responsible for subrecipient monitoring, Epidemiology and OHE were unable to provide evidence that staff reviewed Single Audit or program-specific audit reports for all subrecipients expending $750,000 or more during fiscal year 2024. In addition, OFM did not have a current subrecipient monitoring policy and procedure in place to detect subrecipients that met the audit threshold. Health last updated its subrecipient monitoring policy in 2014. Without obtaining the appropriate reports, Health is unable to show it is meeting the requirements set forth in 2 CFR part 200, subpart F, which includes issuing a management decision on audit findings within six months after receipt of the subrecipient's audit report and ensuring that the subrecipient takes timely and appropriate corrective action on all audit findings.

OFM should update its subrecipient monitoring policy and communicate the policy to the applicable offices and districts. In addition, OFM should periodically review the Clearinghouse to determine whether subrecipients who meet the audit threshold obtain the required audits, and that the applicable offices or districts are reviewing the audit reports and considering the impact of any deficiencies identified in audit findings. Epidemiology and OHE should ensure staff review Single Audit or program-specific audit reports for subrecipients who meet the audit threshold and should adhere to all federal requirements when conducting monitoring over such subrecipients.

Strengthen Controls over FFATA Reporting
Type: Internal Control and Compliance
Severity: Significant Deficiency

Health is not completing Federal Funding Accountability and Transparency Act (FFATA) reporting for the ELC and STLT federal grant programs. During our audit, we found that Epidemiology and OHE did not complete FFATA reporting submissions for subrecipients who received $30,000 or more in ELC and STLT funds.

During fiscal year 2024, Health disbursed approximately $11 million in ELC funds and $5.8 million in STLT funds to subrecipients. Title 2 CFR Part 170 Appendix A, included in award documents signed by management, requires Health to report each obligating action, exceeding $30,000, to the FFATA Subaward Reporting System (FSRS). Health's FFATA reporting policy, which Health last updated in 2014, states that all offices and districts that are recipients of federal grants and contracts shall adhere to all requirements of the FFATA and ensure timely and accurate reporting.

Epidemiology and OHE have experienced turnover in key positions that were historically responsible for completing and submitting FFATA reports. In addition, OFM did not have a procedure in place to detect subawards that it should have reported to FSRS. Not reporting to FSRS could result in a citizen or federal official having a distorted view as to how Health is obligating federal funds.

Epidemiology and OHE should ensure program personnel adhere to Health policies and procedures and fulfill FFATA reporting responsibilities by submitting required FFATA subaward reporting information by the due date and retaining documentation to support the submissions. Additionally, OFM should update and communicate the FFATA reporting policy to applicable offices and districts. Further, OFM should periodically analyze subaward records to determine if there are instances where program personnel are not submitting the required FFATA subaward reporting information. If so, OFM should collect this information from the applicable program personnel promptly to comply with the FFATA reporting requirements.

Improve Controls over Employee Offboarding Process
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2023

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

- The Office of Human Resources (Human Resources) was unable to locate the completed separation checklist for 14 of the 25 (56%) terminated employees sampled.

- Human Resources did not record termination dates within the Commonwealth's human resource and payroll management system within five business days for eight of the 25 (32%) terminated employees sampled.

- Human Resources was unable to confirm the collection of state property for 13 of the 23 (57%) terminated employees sampled.

- Human Resources was unable to confirm the removal of system and building access within 24 hours of termination date for 15 of the 25 (60%) terminated employees sampled.

- Two employees continued to receive salary payments for up to 52 days after separation, totaling $13,634 in improper payments.

The Security Standard states an organization must disable information system access within 24 hours of employee separation and terminate any authenticators or credentials associated with the individual. Additionally, Human Resources internal policy states that a separation checklist must be performed upon employee termination. Performing separation checklists immediately upon employee separation provides confirmation of the collection of all Commonwealth property assigned to the employees and increases the likelihood that Health will enter termination dates into the system timely. It also ensures proper removal of access to Health's critical information systems. Not adequately completing the separation checklist increases the risk of misappropriation of Commonwealth assets. According to management, untimely communication between supervisors of several departments to Human Resources creates delays in the employee offboarding process, which impacts other factors such as the removal of system and building access, payroll processing, and the completion of related documentation. In addition, Health does not have adequate and updated internal policies and procedures other than the Commonwealth Accounting Policies and Procedures (CAPP) Manual to address the timeliness of required communication between Human Resources and payroll personnel.

Health should review its current offboarding practices and develop policies and procedures that are reasonable, and that establish effective internal controls. In addition, Health should ensure supervisors and Human Resources complete documentation and make it readily available upon request. Health's management should also notify supervisors, Human Resources, and payroll personnel of the

timeframe required according to such policies and procedures, to ensure that timely communications occur during the offboarding process.

Improve System Access Procedures
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2023

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

- For three of the 15 (20%) sampled accounting and financial reporting system users granted access during the current fiscal year, we found job functions that we consider to be a separation of duties conflict. These users' assigned roles violate the principle of least privilege and OIM was unable to provide compensating control documentation to ensure system access is appropriate.

- For four of the 25 (16%) sampled patient management system users granted access during the current fiscal year, OIM was unable to provide supporting documentation that supervisors properly approved assigned roles. In addition, for six of the 25 (24%) sampled patient management system users granted access during the current fiscal year, OIM was unable to provide supporting documentation showing that the assigned roles agreed to the access requested.

The Security Standard requires the agency to employ the principle of least privilege, allowing only authorized access for users that is necessary to accomplish assigned tasks. Additionally, the Security Standard requires the agency to separate duties of individuals as necessary, document separation of duties of individuals, and define information system access authorization to support the separation of duties. When improper separation of duties exists, there is an increased risk that users can perform unauthorized transactions in Health's accounting and financial reporting system and patient management system. Approved documentation of the separation of duties concerns and compensating controls in place provides accountability and assurance that Health is properly considering the risks of granting such access to its critical information systems. Lastly, not ensuring that system users have and retain appropriate access to Health's critical information systems increases the risk of unauthorized individuals inappropriately entering or approving transactions and could affect the integrity of Health's transactions within its systems.

While Health has documented system access procedures, Health has not identified conflicting roles and does not have written documentation to justify and authorize access to the conflicting roles within its critical information systems when separation of duties concerns exists. Health should update its system access policies to require written documentation for users to justify and authorize conflicting access to its critical information systems. If violating the principle of least privilege and causing separation of duties issues is unavoidable, Health should document the users with roles that cause

separation of duties issues, document the compensating controls in place to mitigate risk, and obtain management approval to achieve compliance with the Security Standard. Lastly, Health should ensure supervisors properly authorize all access roles and retain records of such authorization.

Improve Vulnerability Management

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

Health does not consistently remediate vulnerabilities for software that is under Health's purview within the timeframe required in Health's Risk Assessment Policy document and the Security Standard. The Virginia Information Technologies Agency (VITA) is responsible for remediating vulnerabilities related to servers and endpoints, but Health is responsible remediating vulnerabilities for applications.

Health and VITA work together to scan Health's systems for vulnerabilities. After obtaining and reviewing vulnerability scan reports, Health identifies the vulnerabilities in the reports that are Health's responsibility for remediating and assigns technical staff to remediate each identified vulnerability. However, Health does not ensure that it remediates each vulnerability within the timeframe required in Health's Risk Assessment Policy and the Security Standard. As of October 2024, Health had not applied a significant number of security patches that are critical and highly important to its information technology (IT) environment, all of which are past the 30-day update window required by Health's Risk Assessment Policy and the Security Standard.

Health's Risk Assessment Policy and the Security Standard each state that the organization's Information Security Officer shall remediate legitimate vulnerabilities within 30 days unless otherwise specified by Commonwealth Security Risk Management in accordance with an organizational assessment of risk. Without remediating vulnerabilities within the required timeframe, Health increases the risk of unauthorized access to the IT environment and the likelihood of data breaches. In addition, software vulnerabilities, whether patching or configuration-based, are common flaws used by unauthorized actors to infiltrate a network and initiate an attack, which can lead to financial, legal, and reputational damages for Health.

Resource constraints in the Information Security Office hindered effective end-to-end vulnerability management. Additionally, competing priorities, including operational duties, within the OIM contributed to the increased time from discovery to remediation of legitimate vulnerabilities. Health has been actively working to remediate all vulnerabilities for which it is responsible and is in the process of hiring a resource dedicated to vulnerability management that will assist in the remediation process. Health should dedicate the resources necessary to improve its vulnerability management process and ensure that it remediates vulnerabilities within the timeline required by the Risk Assessment Policy and the Security Standard. By remediating vulnerabilities timely, Health will reduce data security risk for sensitive and mission-critical systems and better protect the confidentiality, integrity, and availability of the data processed by those systems.

Strengthen Controls over System Reconciliations
Type: Internal Control
Severity: Significant Deficiency

OFM has not developed adequate policies and procedures for preparing monthly reconciliations between the Commonwealth's accounting and financial reporting system and Health's accounting and financial reporting system (Health's system). During the fiscal year 2024 audit, we identified the following deficiencies:

- OFM did not provide evidence of sign offs by the preparer or the reviewer for three of the three (100%) monthly reconciliations selected.

- OFM could not provide documentation to show that it had performed a reconciliation for one of the three monthly reconciliations selected (33%).

CAPP Manual Topic 20905 states that, "to ensure accuracy and uniformity in the preparation and reconciliation of financial data input into the Commonwealth's accounting and financial reporting system, all internally prepared accounting records and other accounting data must be reconciled to reports produced by the Commonwealth's accounting and financial reporting system. Such reconciliations shall be performed and certified to Accounts monthly, as described in this CAPP Topic, and at fiscal year-end, as prescribed by the Comptroller's annual fiscal year-end closing procedures memorandum to agencies." In addition, CAPP Manual Topic 20905 further states that "CAPP Manual procedures alone never eliminate the need and requirement for each agency to publish its own internal policy and procedure documents, approved in writing by agency management." Furthermore, CAPP Manual Topic 20905 also states that documentation for such reconciliations must be retained for three years. The lack of adequate internal policies and procedures, customized to reflect the agency's staffing, organization, and operating procedures, reflects inadequate internal control, and it increases the risk that any discrepancies between the Commonwealth's accounting and financial reporting system and Health's system would not be timely identified and addressed.

Key positions in OFM have experienced significant turnover, which led to the issues identified. During the audit period, Health recruited new staff for a role historically responsible for preparing reconciliations. Health filled one of these positions, an accountant responsible for performing monthly reconciliations, in February 2024 after the position being vacant for approximately two years. OFM should develop and implement adequate policies and procedures to prepare monthly reconciliations between the Commonwealth's accounting and financial reporting system and Health's system. These policies and procedures should, at a minimum, include delegating responsible authority for monthly reconciliations, defining a timeframe for preparation and review, defining a timeframe for researching and clearing any reconciling discrepancies, and retaining the preparer and reviewer's signatures and dates. Additionally, OFM should retain and make available, upon request, documentation that confirms the completion of monthly reconciliations in accordance with CAPP Manual Topic 20905.

Strengthen Controls over Procurement
Type: Internal Control and Compliance
Severity: Significant Deficiency

Epidemiology is not compiling and retaining a comprehensive contract listing for all procured and active contracts funded by the ELC federal grant program. Management was unable to provide the comprehensive contract listing due to not properly maintaining the documentation.

Title 2 CFR § 200.317 governs procurements by states and requires that "when procuring property and services under a Federal award, a State must follow the same policies and procedures it uses for procurements from its non-Federal funds." Department of General Services Agency Procurement and Surplus Property Manual (APSPM) - Section 10.3 requires agencies to maintain a complete file in one place for each purchase transaction. It states that the file must contain, at a minimum, as applicable, the description of requirements, sources solicited, a copy of the Virginia Business Opportunities receipt, cancellation notices, the method of evaluation and award, a signed copy of the contract or purchase order, contractor performance report submitted by the administrator, modifications or change orders, vendor complaint forms, cure letters, usage data such as release or obligation registers, and any other actions relating to the procurement. In addition, APSPM Annex 10-A, which is a Post Award Administration Checklist, requires the agency to list the contract on the agency's master contract list or schedule to include period of performance and any renewal option(s) to allow for the planning of renewal or rebidding actions.

Health's individual offices or Local Health Districts (LHD) complete procurements for the ELC federal grant program up to $100,000, with procurements over $10,000 and up to $100,000 being solicited through a "quick quote." Health's Office of Procurement and General Services handles complex procurements. Since Health has 35 LHDs, the absence of a comprehensive contract listing increases the risk of a contract being established by an LHD that goes unnoticed by Epidemiology. Due to limited staff and the number of health offices and LHDs involved in the procurement process, Epidemiology was unable to provide a comprehensive contract listing. By not maintaining proper documentation and support, Health is unable to ensure the effectiveness of internal controls. Furthermore, it is difficult to substantiate the legitimacy of the procurement transaction, increasing the risk of unauthorized transactions, which also increases the potential for questioned costs.

Health's management should develop a policy requiring the compilation of comprehensive contract listings and communicate the policy to the applicable offices and districts. Health's management should also ensure that the applicable offices and districts involved have adequate staffing and training on contract procurement and the need to maintain adequate documentation for all procurements.

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

Health continues to not conduct a comprehensive IT security audit on each sensitive system at least once every three years that assesses whether IT security controls are adequate and effective. Health made significant progress by completing an IT Security Audit on 26 of its 54 sensitive systems in the last three years. However, Health has not conducted a comprehensive IT security audit on the remaining 28 sensitive systems in the last three years.

The Security Standard requires that each IT system classified as sensitive undergo an IT security audit as required by and in accordance with the current version of the Commonwealth's IT Security Audit Standard, SEC502 (IT Audit Standard). The IT Audit Standard requires that IT systems containing sensitive data, or systems with an assessed sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall receive an IT security audit at least once every three years. Additionally, the IT Audit Standard requires that the IT Security Auditor shall use criteria that, at a minimum, assess the effectiveness of the system controls and measure compliance with the applicable requirements of the Security Standard.

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

The Office of Internal Audit (OIA) Administrative Procedures (OIA Procedures) tasks OIA with performing IT security audits. Although Health hired two IT Security Auditors within OIA to perform IT security audits of sensitive systems, the magnitude of the project required Health to also hire a contractor to complete the audits. Despite filling these positions, time and budgetary constraints continue to contribute to OIA's delay in performing the remaining technical audits of sensitive systems or procuring an external auditor to complete the required audits. Additionally, since 2017, Health has not reviewed and revised its OIA Procedures to ensure the policy details the necessary requirements and processes to facilitate completing IT Security Audits timely. Finally, OIA's current IT Audit Plan does not include each of the sensitive systems on the list of sensitive systems maintained by OIM.

OIA should update its OIA Procedures to detail the necessary requirements and document its process for conducting IT audits over each sensitive system at least once every three years. OIA should coordinate with OIM to obtain a comprehensive sensitive systems list to ensure the IT Audit Plan includes each sensitive system. Health should then complete the necessary IT security audits, either through OIA or through the acquisition of continued external third-party services. Compliance with the IT Audit Standard will help to ensure the confidentiality, integrity, and availability of sensitive and mission-critical data.

Develop Required Information System Policies and Procedures

Type: Internal Control and Compliance

Severity: Significant Deficiency

Health does not have documented policies and procedures for all control families as required by the Security Standard. Specifically, Health does not have documented policies and procedures for the following three control families:

- PE - Physical and Environmental Protection
- PM – Program Management
- SI – System and Information Integrity

The Security Standard requires Health to document an organization-level policy over each control family and to document procedures to facilitate the implementation of the policy. The Security Standard also requires Health to review and update the policies and procedures annually. Without developing and implementing policies and procedures for each control family as required by the Security Standard, Health cannot ensure that it has documented the necessary control requirements to address security needs across its IT environment. Without documented control requirements, Health risks not implementing adequate controls which could result in the compromise of sensitive and mission critical data.

Management oversight at OIM resulted in the lack of documented policies and procedures for these control families. Additionally, Health does not have a process in place to document all policies and ensure it maintains a policy for each control family as required by the Security Standard. Health should develop, document, and disseminate to the appropriate organization-defined personnel an organization-level policy and procedure for all control families. Once Health has developed the policies and procedures, Health should review the documents on an annual basis. Taking these actions will help Health ensure the confidentiality, integrity, and availability of its sensitive and mission-critical data.

RISK ALERT

During our audit, we encountered issues that are beyond the corrective action of Health's management alone and which require the action and cooperation of management and VITA. The following issues represent such a risk to Health 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, operations, and support of IT infrastructure components, such as servers, routers, firewalls, and virtual private networks. Health continues to rely on contractors procured by VITA for the installation of security patches in systems that support Health's operations. Additionally, Health relies on VITA as the contract administrator to maintain oversight and enforce the contract agreements with the ITISP contractors. As of October 2024, the ITISP contractors had not applied a significant number of security patches that are critical and highly important to Health's 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 Health's IT infrastructure to remediate vulnerabilities in a timely manner or take actions to obtain these required services from another source. Additionally, our separate audit of VITA's contract management will also continue to report on this issue.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

Febuary 7, 2025

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Janet Kelly
Secretary of Health and Human Resources

Karen Shelton, MD
State Health Commissioner

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

Audit Objectives

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

Audit Scope and Methodology

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

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

- Accounts receivable
- Collection of fees for services
- Commonwealth's retirement benefits system
- Cooperative agreements between Health and local governments, including:
  - Accounts payable
  - Aid to and reimbursement from local governments
- Donated Inventory
- Eligibility for:
  - Special Supplemental Nutrition Program for Women, Infants and Children
- Emergency medical services revenues
- Federal revenues, expenses, and compliance for the following federal grant programs:
  - Activities to Support State, Tribal, Local and Territorial (STLT) Health Department Response to Public Health or Healthcare Crises
  - Coronavirus State and Local Fiscal Recovery Funds
  - Drinking Water State Revolving Fund
  - Epidemiology and Laboratory Capacity Program for Infectious Diseases
- Information system security (including access controls)
- Payroll expenses

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

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

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

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements or noncompliance on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements or material noncompliance with a type of compliance requirement of a federal program will not be prevented or detected and corrected on a timely basis. We consider the deficiency titled "Strengthen Controls over Financial Reporting," which is described in the section titled "Internal Control and Compliance Findings and Recommendations," to be a material weakness.

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 consider the remaining deficiencies described in the section titled "Internal Control and Compliance Findings and Recommendations," to be significant deficiencies.

Conclusions

We found that Health properly stated, in all material respects, the amounts recorded and reported in the Commonwealth's accounting and financial reporting system, Health's accounting and financial reporting system, and supplemental information and attachments submitted to Accounts, after adjustment for the misstatements noted in the finding "Strengthen Controls over Financial Reporting."

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."

Health has taken adequate corrective action with respect to two 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 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, 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 30, 2025. Government Auditing Standards require the auditor to perform limited procedures on Health's response to the findings identified in our audit, which is included in the accompanying section titled "Agency Response." Health's response was not subjected to the other auditing procedures applied in the audit and, accordingly, we express no opinion on the response.

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

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

AVC/clj

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	First Reported for Fiscal Year
Follow Eligibility Documentation Requirements for Women, Infants, and Children Program	Complete	2021
Improve Controls over Journal Entries	Complete	2022
Strengthen Controls over Financial Reporting	Ongoing	2021
Continue Strengthening the System Access Removal Process	Ongoing	2014
Review Subrecipient Audit Reports	Ongoing	2024
Strengthen Controls over FFATA Reporting	Ongoing	2024
Improve Controls over Employee Offboarding Process	Ongoing	2023
Improve System Access Procedures	Ongoing	2023
Improve Vulnerability Management	Ongoing	2023
Strengthen Controls over System Reconciliations	Ongoing	2024
Strengthen Controls over Procurement	Ongoing	2024
Conduct Information Technology Security Audits	Ongoing	2023
Develop Required Information System Policies and Procedures	Ongoing	2024

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

COMMONWEALTH of VIRGINIA
Department of Health
Karen Shelton, MD
State Health Commissioner
P O BOX 2448
RICHMOND, VA 23218
TTY 7-1-1 OR
1-800-828-1120

February 4, 2025

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

Dear Ms. Henshaw:

The Virginia Department of Health has reviewed your audit report for the period ending June 30, 2024. We concur with the findings and our corrective action plan will be provided in accordance with the Department of Accounts guidelines.

We appreciate your team's efforts and constructive feedback. If you have any additional questions, please contact Tasha Owens, Internal Audit Director, at 804-864-7450 or tasha.owens@vdh.virgina.gov.

Sincerely,

Karen Shelton, MD
State Health Commissioner

VDH VIRGINIA DEPARTMENT OF HEALTH