


DEPARTMENT OF HEALTH

REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2025

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: WIC Special Supplemental Nutrition Program for Women, Infants, and Children; and Immunization Cooperative Agreements, for the fiscal year ended June 30, 2025, 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);

- one matter involving internal control and its operation requiring management's attention; however, we do not consider it to be a material weakness;

- eight matters involving internal control and its operation requiring management's attention that also represent instances of noncompliance with applicable laws and regulations that are required to be reported under Government Auditing Standards; and

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

Additionally, our 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 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 recommendation.

-TABLE OF CONTENTS–

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

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

The Department of Health (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 nine of the 25 (36%) terminated employees sampled.

- Human Resources was unable to confirm the collection of state property for nine of the 25 (36%) terminated employees sampled.

- Human Resources was unable to confirm the removal of system and building access within 24 hours of termination date for nine of the 25 (36%) terminated employees sampled.

- Health did not remove system access timely for 14 out of 482 (3%) terminated users of Health's accounting and financial reporting system. Health removed these accounts nine to 206 days after the associated employee's termination date.

- Health did not remove system access timely for 38 out of 211 (18%) terminated users of Health's patient management system. Health removed these accounts three to 61 days after the associated employee's termination date.

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. 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 did not have adequate and updated internal policies and

procedures effective during fiscal year 2025, other than the Commonwealth Accounting Policies and Procedures (CAPP) Manual, to address the timeliness of required communication between Human Resources and payroll personnel.

During fiscal year 2025, Health created a new policy, conducted additional training for Human Resources personnel, and implemented a new system where supervisors will submit employee offboarding notifications. However, these new policies and procedures, as well as the new system, were not in effect or fully operational for the entire fiscal year. Health should ensure the system implemented requires adequate documentation to satisfy internal controls relating to offboarding; supervisors and Human Resources complete all required documentation within the new system; and that documentation is readily available upon request. Health's management should also notify supervisors, Human Resources, and payroll personnel of the timeframe required for access removal per Health's policies and procedures and the Security Standard to ensure that timely communications occur during the offboarding process.

Improve Controls over Overtime
Type: Internal Control
Severity: Significant Deficiency

Human Resources does not have a formal process to periodically monitor employee overtime. During our audit, we reviewed all employees who received overtime compensation exceeding 20 percent of their regular pay. The six employees reviewed had individual overtime up to $27,030 or 38.6 percent of their regular pay during fiscal year 2025, with total overtime hours per employee ranging from 213 to 764 hours. These employees work in five different Health locations, with two from the same district.

The Commonwealth's Department of Human Resource Management *Policy No. 1.25 – Hours of Work* states that "agency management should limit overtime assignments to situations where it is necessary," and that "employees may work overtime hours only as authorized in advance by his or her supervisor or manager." While supervisors electronically approved all employee timesheets when submitted and provided reasonable justifications for the overtime when requested during the audit, Human Resources does not have a centralized oversight process in place, including a routine monitoring process, to ensure overtime hours are reasonable and excessive hours are appropriately justified.

Health's time and attendance system allows supervisors to attach supporting documentation to timesheets showing overtime approval; however, Health does not require supporting documentation, and supervisors did not consistently provide such documentation. In some cases, supervisors used general approval language when approving timesheets rather than attaching specific authorization or justification. Such generalized approvals may reflect an increased risk of management oversight. The absence of monitoring and detective internal controls increases the risk that Human Resources may not identify instances where supervisors are not properly tracking overtime and ensuring overtime hours are

justified as being necessary and creates a risk for potential misuse or abuse of overtime without timely detection or corrective action.

Human Resources should establish a formal process to periodically monitor employee overtime and identify any excessive overtime or unusual patterns. This process should document periodic inquiries with the applicable supervisors to ensure that all overtime is necessary, reasonable, and properly authorized. Additionally, Human Resources should ensure staff consistently complete and maintain supporting documentation for overtime approvals and justifications, and that this documentation is readily available upon request. To strengthen accountability, Human Resources should also train supervisors to increase awareness of their responsibilities related to overtime tracking and reporting so they are prepared to provide timely and accurate explanations when needed.

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

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

Health and VITA work together to scan Health's systems for vulnerabilities. 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 August 2025, Health had not applied 40 security patches that were critical and highly important to its information technology environment, all of which were past the 30-day update window allowed 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 information technology (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.

Although Health has made progress since the prior year in remediating vulnerabilities, resource constraints in the Office of Information Security (OIS), including staff reductions in the past year, continue to hinder Health's ability to remediate vulnerabilities. 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.

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. While Health established an IT Audit Plan during the fiscal year, Health has not conducted a comprehensive IT security audit of 32 of its 59 (54%) 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 systems containing sensitive data, or systems with an assessed sensitivity of high on any of the criteria of confidentiality, integrity, or availability, receive an IT security audit at least once every three years. Additionally, the IT Audit Standard requires that the IT Security Auditor use criteria that, at a minimum, assess the effectiveness of the system controls and measure compliance with the applicable requirements of the Security Standard. Further, the Office of Internal Audit (OIA) *Administrative Procedures – Subject 7: IT Security Audits* (OIA Procedures) require audits of each sensitive IT system be conducted on a three-year rotational basis in accordance with the IT Audit 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.

During the fiscal year, Health made progress to update its OIA Procedures to detail the necessary requirements and document its process for conducting IT security audits over each sensitive system at least once every three years. Additionally, Health created an IT Audit Plan which includes Health's sensitive systems and schedules for each to receive an audit at least once every three years; however, Health did not include all systems classified as sensitive in its IT Audit Plan and did not complete one of

the 12 planned IT security audits. Continued time and budgetary constraints, turnover, and miscommunication between OIA and the Office of Information Management (OIM) contributed to OIA's delay in performing the remaining technical audits of sensitive systems.

OIA should coordinate with OIM to obtain a comprehensive list of sensitive systems to ensure the IT Audit Plan is complete. Health should then dedicate the resources necessary to conduct IT security audits over any sensitive systems exceeding the three-year requirement. Compliance with the OIA Procedures and 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
First Reported: Fiscal Year 2024

Health does not have documented procedures for all control families as required by the Security Standard. During fiscal year 2025, Health developed documented policies for all control families, as well as documented procedures for the Program Management control family; however, Health has not documented procedures for the Physical and Environmental and the System and Information Integrity control families.

The Security Standard requires Health to document procedures over each control family to facilitate the implementation of the organization-level policies. The Security Standard also requires Health to review and update the procedures annually. Without developing and implementing procedures for each control family as required by the Security Standard, Health cannot ensure that it consistently complies with the control requirements documented in its policies, which increases the risk of compromising sensitive and mission-critical data.

The lack of documented procedures in all control families resulted from management oversight by OIM during the approval process. Health should develop, document, and disseminate to the appropriate organization-defined personnel an organization-level procedure for the remaining two control families. Once Health develops the procedures, it 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.

Improve Threat Management and Incident Response Program

Type: Internal Control and Compliance
Severity: Significant Deficiency

Health's threat management and incident response program does not include certain elements required by the Security Standard and Health's Incident Response Policy. Additionally, Health does not include all required elements in its Incident Response Policy. Specifically, the following weaknesses exist:

- Health's Incident Response Form does not require employees to report information security incidents to the Chief Information Security Officer (CISO) and system owners in accordance with the Incident Response Policy.

- Health does not ensure employees report information security incidents within 24 hours in accordance with the Incident Response Policy and the Security Standard.

- Health has not developed and documented an Incident Response Plan. Additionally, the Incident Response Policy does not include all elements required by the Security Standard for an Incident Response Plan.

- Health has not developed threat detection and incident response documentation including threat detection practices, monitoring and logging procedures, and mitigation procedures in accordance with the Incident Response Policy and the Security Standard.

- Health does not review and update its Incident Response Policy on an annual basis in accordance with the Incident Response Policy and the Security Standard.

Incorrect instructions on Health's Incident Response Form, resource constraints, competing priorities, and management oversight contributed to Health not including all required elements for an Incident Response Plan, not documenting and implementing all elements of the Incident Response Policy, and not reviewing the Incident Response Policy annually. Without documenting and implementing the necessary and required elements in its threat management and incident response program, Health may inconsistently implement the incident response program and increase the risk of mismanaging security incidents.

Health should ensure that its employees report incidents to the correct individuals within 24 hours. Health should also update the Incident Response Policy to include all required Incident Response Plan elements, then prioritize developing and documenting an Incident Response Plan. Additionally, Health should develop documentation for threat detection practices, monitoring and logging procedures, and mitigation procedures. Finally, Health should review and update the Incident Response Policy annually. Improving the threat management and incident response program will help ensure the agency

appropriately responds to malicious attempts to compromise confidentiality, integrity, and availability of sensitive information.

Improve Web Application Security
Type: Internal Control and Compliance
Severity: Significant Deficiency

Health does not secure the web application, which supports its system used for eligibility determination for the WIC Special Supplemental Nutrition Program for Women, Infants, and Children federal grant program, with the minimum-security controls required by the Security Standard. We communicated the weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

The weaknesses identified resulted from limited management oversight and staffing constraints within OIM. Health should dedicate the resources necessary to develop and maintain adequate documentation and implement all security controls required by the Security Standard. Addressing these weaknesses will help ensure the confidentiality, integrity, and availability of data and support compliance with the Security Standard.

Improve Change Control and Configuration Management Process
Type: Internal Control and Compliance
Severity: Significant Deficiency

Health's change control and configuration management process does not meet certain minimum requirements contained in its Configuration Management Policy (Configuration Policy), as well as the Security Standard resulting in the following weaknesses:

- Health does not perform an annual review of its Configuration Policy.
- Health does not document formal procedures to facilitate the implementation of the Configuration Policy and associated configuration management controls. As a result, there are no formal procedures which detail the following change control processes:
    - Determining and documenting the types of changes that are configuration controlled.
    - Recording and tracking change requests through the lifecycle of the change.
    - Analyzing changes to the system to determine potential security and privacy impacts prior to change implementation for software development changes.

- Testing, validating, and documenting changes to the system before implementing the change in the production environment.

- Reviewing and approving or disapproving of proposed changes by a Change Control Board or another governing authority.

- Ensuring only authorized individuals develop software development changes.

- Monitoring and reviewing activities associated with configuration-controlled changes.

Without performing an annual review of its Configuration Policy and documenting formal procedures, Health may not implement and communicate the controls and processes needed to maintain a secure change control and configuration management process. As a result, Health is at a higher risk for implementing unauthorized changes to its production environment and negatively affecting the confidentiality, integrity, and availability of its sensitive systems and data.

Resource constraints, as well as a reliance on high-level workflow diagrams, resulted in the above weaknesses. Health should perform an annual review of its Configuration Policy, as well as develop and document formal configuration and change management procedures that align with the requirements in the Configuration Policy and the Security Standard. By implementing these controls, Health will reduce the risk of unauthorized changes in the environment and will help improve the confidentiality, integrity, and availability of mission-critical and sensitive systems.

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

Health has not implemented a security awareness and training (SAT) program in accordance with its Information Security Awareness and Training Policy and Procedures (Training Policy), the Security Standard, and the Commonwealth's Security Awareness Training Standard, SEC527 (Training Standard). The Security Standard requires Health's CISO to develop and maintain a SAT program, which is critical to ensuring that users understand their roles and responsibilities in securing sensitive information within Health. During our review, we found the following weaknesses:

- Health does not annually review and update its Training Policy.

- Health failed to ensure that each user completed the required new hire, annual, and/or role-based training, resulting in the following noncompliance rates:

  - Eight out of 24 (33%) system and data owners did not complete the required training.

- Two out of eight (25%) application and system administrators did not complete role-based training.

- Eight out of 33 (24%) non-Health users did not complete the 2024 cybersecurity HIPAA awareness training.

- 20 out of 120 (17%) Health users did not complete the cybersecurity HIPAA awareness training.

- 158 out of 930 (17%) new hires did not complete the new hire cybersecurity awareness training.

- 182 out of 2,928 (6%) users did not complete the annual cybersecurity awareness training.

- Health did not ensure users completed remedial training, when required. We found the following noncompliance rates:

  - 125 out of 1,139 (11%) users who failed one phishing exercise did not complete the required remedial training.

  - 34 out of 337 (10%) users who failed two phishing exercises did not complete the required remedial training.

  - Seven out of 74 (9%) users who failed more than two phishing exercises did not complete the required remedial training.

The Security Standard requires Health to maintain updated awareness and training documentation and implement an adequate SAT program. By not conducting annual policy reviews and ensuring users complete required training, Health cannot ensure that it has effectively communicated, implemented, and enforced security controls and process requirements. As a result, Health elevates the risk of human error and malicious users exploiting potential gaps in the IT environment. Systems susceptible to cybersecurity threats could lead to significant security breaches within Health's environment.

Resource constraints within OIS impacted Health's ability to perform an annual review and update of its Training Policy. Additionally, due to turnover, the security training platform (STP) administrator position was vacant for a significant portion of the fiscal year under review, which impacted Health's ability to effectively administer the security awareness training program to ensure compliance. While Health informs users of training deadlines and sends reminders, it does not enforce completion through a formal enforcement mechanism. This lack of enforcement has further contributed to noncompliance among users required to complete the training.

Health should review and update its Training Policy to correspond with current Health security awareness and education practices and complete a review of this policy annually. Additionally, Health's CISO and the STP administrator should oversee the STP to ensure SAT completion. Furthermore, Health should establish and implement a process for handling noncompliant users that includes a formal enforcement mechanism. Addressing these weaknesses will help protect Health from malicious attempts that could compromise the confidentiality, integrity, and availability of sensitive and mission-critical data.

RISK ALERT

During our audit, we encountered an issue that is beyond the corrective action of Health's management alone and which requires the action and cooperation of management and VITA. The following issue represents such a risk to Health and the Commonwealth.

Unpatched Software

First Reported: Fiscal Year 2021

VITA contracts with various providers, collectively known as 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. 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 August 2025, the ITISP contractors had not applied a significant number of two 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. Health 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.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

Janaury 16, 2025

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Janet Kelly
Secretary of Human and Health 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, 2025. 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, 2025. 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 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
- Emergency medical services revenues
- Federal revenues, expenses, and compliance for the following federal grant programs:
  - WIC Special Supplemental Nutrition Program for Women, Infants, and Children
  - Immunization Cooperative Agreements
- 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. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We identified certain deficiencies in internal control titled "Improve Controls over Employee Offboarding Process," "Improve Controls over Overtime," "Improve Vulnerability Management," "Conduct Information Technology Security Audits," "Develop Required Information System Policies and Procedures," "Improve Threat Management and Incident Response Program," "Improve Web Application Security," "Improve Change Control and Configuration Management Process," and "Improve Security Awareness Training Program," 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 or noncompliance on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements or material noncompliance with a type of compliance requirement of a federal program will not be prevented or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

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.

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 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" 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, 2025. The Single Audit Report will be available at www.apa.virginia.gov in February 2026.

Exit Conference and Report Distribution

We discussed this report with management at an exit conference held on January 29, 2026. 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/vks

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	Fiscal Year First Reported
Continue Strengthening the System Access Removal Process	Complete	2014
Strengthen Controls over Financial Reporting	Complete	2021
Improve System Access Procedures	Complete	2023
Strengthen Controls over System Reconciliations	Complete	2024
Improve Controls over Employee Offboarding Process	Ongoing	2023
Improve Controls over Overtime	Ongoing	2025
Improve Vulnerability Management	Ongoing	2023
Conduct Information Technology Security Audits	Ongoing	2023
Develop Required Information System Policies and Procedures	Ongoing	2024
Improve Threat Management and Incident Response Program	Ongoing	2025
Improve Web Application Security	Ongoing	2025
Improve Change Control and Configuration Management Process	Ongoing	2025
Improve Security Awareness Training Program	Ongoing	2025
Review Subrecipient Audit Reports**	Ongoing	2024
Strengthen Controls over FFATA Reporting**	Ongoing	2024
Strengthen Controls over Procurement**	Ongoing	2024

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

**These audit findings originated from the fiscal year 2024 audit of the Epidemiology and Laboratory Capacity for Infectious Diseases and the Activities to Support State, Tribal, Local and Territorial Health Department Response to Public Health or Healthcare Crises federal grant programs. These federal grant programs are out of scope for the Commonwealth's 2025 Single Audit, and as such, we limited our audit procedures to confirming the accuracy of the corrective action statuses in the Commonwealth's Summary Schedule of Prior Audit Findings. Per inquiry with Health's management, we determined that corrective action was ongoing for these audit findings as of June 30, 2025.

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

B. Cameron Webb, MD, JD
State Health Commissioner

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

February 4, 2026

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, 2025. 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 804-864-7450or tasha.owens@vdh.virginia.gov.

Sincerely,

Dr. Cameron Webb
State Health Commissioner

VDH VIRGINIA DEPARTMENT OF HEALTH