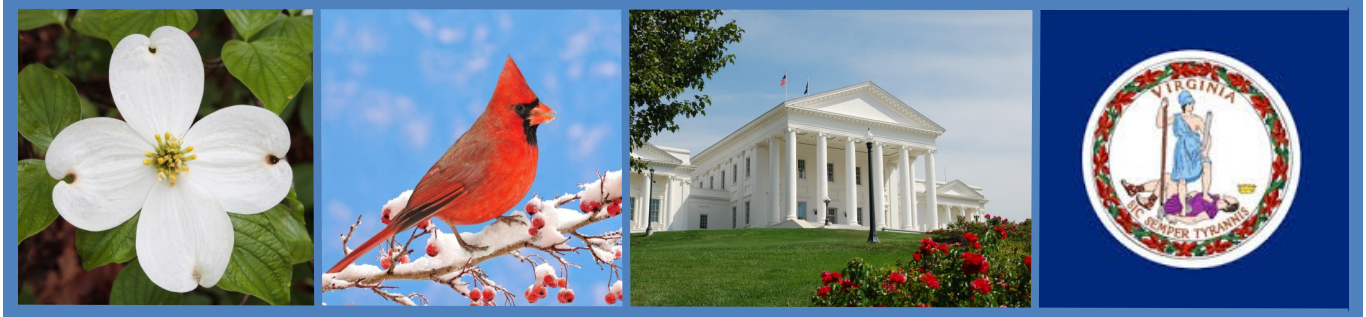

VIRGINIA EMPLOYMENT COMMISSION

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 Virginia Employment Commission (Commission) for the year ended June 30, 2025, found:

- proper recording and reporting of all transactions, in all material respects, in the Commonwealth's accounting and reporting system, the Commission's benefits and tax, and financial systems, and the enterprise fund template submitted to the Department of Accounts (Accounts) after adjustment for the misstatements noted in the finding "Improve Internal Controls over the Collection and Reporting of Accounts Receivable";

- one deficiency related to the collection and reporting of accounts receivable that we consider to be a material weakness in internal control;

- seven additional 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; however, we do not consider the matters to be material weaknesses; and

- adequate corrective action with respect to the prior audit finding 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 recommendation.

-TABLE OF CONTENTS-

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Internal Controls over the Collection and Reporting of Accounts Receivable
Type: Internal Control
Severity: Material Weakness

The Commission does not have adequate controls over the reporting and collection of certain receivables. The Commission's Finance Division (Finance) is responsible for submitting accounts receivable balances to the Department of Accounts (Accounts) in a timely manner for use in preparing the Commonwealth's financial statements. Additionally, the Commission is responsible for actively pursuing amounts due to the Commonwealth. During our review of accounts receivable, we identified the following issues:

- Finance's initial reporting to Accounts included a negative $37.6 million in receivables for unemployment overpayments, which incorrectly portrayed that the Commission owes a material amount in unemployment benefits to claimants.

- The Commission has continued to report $2.8 million as due from other states since the pandemic; however, has not taken steps to pursue collection on these accounts.

- The Commission did not provide corrected fiscal year end accounts receivable balances to Accounts until the first week of December; which is three months after the due date set by Accounts and over five months after fiscal year end.

The Commission's responsibilities for receivables are governed by several authoritative sources. The Commonwealth's financial statements must be prepared in accordance with Generally Accepted Accounting Principles (GAAP), which require accurate and timely reporting of financial data as of fiscal year end. Further, the Code of Virginia § 2.2-4800 requires agency management to actively pursue the collection of receivables to ensure that funds owed to the Commonwealth are recovered and available to support ongoing operations. To aid agencies in managing and meeting these requirements, the Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic No. 20505, issued by Accounts, mandates quarterly reporting of accounts receivable by all state agencies, including the Commission. These requirements collectively establish the expectation that the Commission must actively pursue collection and produce and maintain accurate, timely, and complete accounts receivable records for reporting.

Delays in providing accurate accounts receivable information hinder Accounts ability to prepare the Commonwealth's financial statements by the required deadline. Inaccurate or incomplete reporting increases the risk of material misstatements in the Commonwealth's financial statements, which could undermine public trust and financial transparency. Additionally, inaccurate records may limit the Commission's ability to actively pursue collection, which may cause the Commonwealth to lose access to funds that are critical for supporting operations.

One factor contributing to the issues identified was the recent leadership transition within the Finance Division, which, combined with limited documentation of related processes, created challenges in ensuring consistent collaboration between divisions responsible for accounts receivable collection and reporting. Although the Commission reports accounts receivable as a single figure for financial reporting purposes, the underlying balances are derived from six receivable categories and are managed by three distinct internal divisions, each governed by different operational and regulatory frameworks. Significant receivable categories include amounts due from other states, employer tax receivables, reimbursable unemployment claims, and overpayment recoveries from claimants. During the pandemic, the Commission recorded receivables from other states; however, because the Commission did not formally assign responsibility for collection of these receivables, it has not actively pursued collection or confirmed that the other states still owe these amounts. Employer tax receivables included significantly aged balances, some over three years old, that the Commission did not properly evaluate for collectability or adjust through allowances. While the Commission managed reimbursable claims, it made material corrections to claimant overpayment data due to prior reporting errors without completing its investigation of the causes of those errors. The lack of documented procedures to aid in coordination among the internal divisions and insufficient scrutiny of the economic value of receivables contributed to the delays and inaccuracies in reporting.

The Commission should establish formal documented processes for collaboration among all internal divisions responsible for managing receivables including assignment of responsibilities, regular assessments of collectability, and the timely development of allowance estimates based on aging and historical collection trends. Prior to submitting information to Accounts to meet year end reporting deadlines, the Commission should review and validate all receivable data to ensure it is properly supported. Additionally, the Commission should continue to investigate the causes of prior reporting errors and implement corrective actions to prevent recurrence. Further, staff responsible for accounts receivable management should receive training and guidance to reinforce the importance of timely collection, accurate reporting, and compliance with applicable financial reporting standards.

Allocate and Align Resources to Reduce IT Security Risk
Type: Internal Control and Compliance
Severity: Significant Deficiency

The Commission does not allocate and align the necessary resources needed to govern its information security program and address outstanding security control weaknesses to reduce information technology (IT) related risks. The improper allocation of resources has resulted in unresolved information security findings issued by a federal agency, the Commission's Internal Audit Department (Internal Audit), and our audits. Specifically, the Commission has the following number of unresolved findings:

- 326 unresolved findings a 2023 federal agency review identified related to restricting access to authorized individuals and computer systems security.

- 28 unresolved information security findings Internal Audit identified through security audits performed over the last two years. Internal Audit identified seven of the 28 findings in fiscal year 2024 and the remaining 21 findings in fiscal year 2025.

- Five unresolved IT findings from our audits, including one from fiscal year 2023 and four from fiscal year 2024.

The Commonwealth's IT Security Standard, SEC530 (Security Standard) requires agency heads to maintain an information security program that is sufficient to protect the agency's IT system and to ensure the information security program is documented and effectively communicated. The Tax Information Security Guidelines for Federal, State and Local Agencies requires all systems receiving, processing, storing, or transmitting federal information to meet federal computer security requirements and U.S. Department of Treasury directives for configuring minimum security controls.

Without allocating and aligning the appropriate resources to establish oversight and to assess and govern its IT resources and projects to ensure the Commission adheres to the Security Standard, the Commission will not be able to resolve its IT findings in a timely manner to maintain adequate controls to protect its confidential and mission critical data. Additionally, without completing corrective actions, the Commission risks maintaining gaps in key security control areas, which with the passage of time, makes it more susceptible to attacks and data breaches.

Throughout the fiscal year the Commission has been working to conduct comprehensive enterprise-wide and departmental reviews to modernize organizational structures, technology governance, and risk management practices. The Commission determined that significant structural changes were necessary in both Information Technology and Information Security divisions, prompting a full restructuring of the Information Security Office, and redesign of roles and responsibilities. As a result, strategic planning and organizational realignment occurred throughout the fiscal year. The Commission held vacant or redesigned many legacy roles to align with the agency's modernization strategy and strengthen its governance model. These changes to divisions currently assigned responsibility for protecting the Commission's IT systems have delayed the Commission's ability to remediate weaknesses information security audits identified within a reasonable timeframe.

During management's efforts to change the Commission's organizational structure, technology governance, and risk management practices, management should align sufficient resources with responsibilities to implement and maintain information security controls. Because it will involve multiple divisions within the Commission to address the control deficiencies identified in the audit reports mentioned above, management should ensure there is collaboration between the divisions in making revisions as necessary to implement the Commission's corrective action plan. Taking these corrective actions will assist the Commission to protect the confidentiality, integrity, and availability of its sensitive and mission critical data.

Improve IT Risk Management and Contingency Planning Program
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2024

The Commission has made progress in remediating four of the nine weaknesses we previously reported for conducting and maintaining its IT risk management and contingency planning documents in accordance with the Security Standard. Risk management documents include the Commission's Business Impact Analysis (BIA), IT System and Data Sensitivity Classifications (Sensitivity Classifications), IT System Risk Assessments (RA), and System Security Plans (SSP). Contingency planning documents include the Commission's Continuity of Operations Plan (COOP) and Disaster Recovery Plan (DRP). The following five weaknesses remain:

- While the Commission made progress to define its procedures for conducting a BIA and SSPs and to use its BIA as the primary input to its Sensitive Classifications, RA, COOP, and SSPs, the Commission continues not to include Security Classifications based on confidentiality, integrity, and availability within its procedures. By not ensuring its procedures align with the Security Standard, the Commission is unable to consistently identify, conduct, and enforce processes to maintain current risk management and contingency documents.

- The Commission does not conduct a RA for each of its 20 active sensitive systems. The Security Standard requires the Commission to conduct and document a RA for each system classified as sensitive as needed, but not less than once every three years. Without current and complete RAs, the Commission may not detect potential risks and vulnerabilities that can affect its IT environment, which may lead to the Commission not implementing appropriate security controls to mitigate a malicious user from compromising its systems and data.

- The Commission has not developed a SSP for eight of its 20 (40%) active sensitive systems and does not include certain elements for the remaining 12 (60%) SSPs. The Security Standard requires the Commission to develop a SSP for each system that includes several requirements. Each SSP is required to include an overview of the security and privacy requirements for the system and the security and privacy-related activities affecting the system that require planning and coordination with organization-defined individuals or groups.

- The Commission is not conducting nor documenting annual reviews of its RAs and SSPs in accordance with the Security Standard. The Security Standard requires the Commission to conduct these annual reviews to validate the RAs and SSPs are accurate and revised as needed to reflect the Commission's current IT environment. By not reviewing and updating IT risk management and contingency planning documents, the Commission increases the risk that documentation does not reflect its current environment and may delay recovery processes in the event of a disaster or disruption.

- The Commission is not appropriately distributing updated versions of its COOP to executive leadership and key personnel. Without communicating contingency plans to key personnel,

the Commission increases the risk of inconsistent contingency responses, which could result in a delayed response and misaligned actions.

Without completing, maintaining, testing, and updating the IT risk management and contingency planning documents, the Commission increases the risk for ineffective incident response, operational disruption, and data loss. Additionally, without appropriate collaboration amongst the necessary business and IT divisions, the essential staff may not have the most current IT contingency planning documentation in the event emergency procedures are activated.

Throughout the fiscal year the Commission has been working to conduct comprehensive enterprise-wide and departmental reviews to modernize organizational structures, technology governance, and risk management practices. The Commission determined that significant structural changes were necessary in both Information Technology and Information Security divisions, prompting a full restructuring of the Information Security Office, and redesign of roles and responsibilities. As a result, strategic planning and organizational realignment occurred throughout the fiscal year. The Commission held vacant or redesigned many legacy roles to align with the agency's modernization strategy and strengthen its governance model. These changes occurring throughout the fiscal year contributed to the Commission's inability to correct the remaining weaknesses.

Whether the Commission is operating in a period of organizational stability or undergoing intentional structural changes, it needs to continue improving its policies and procedures to ensure they include Sensitivity Classification requirements as defined in the Security Standard. The Commission should complete a RA and SSP for each of its sensitive systems. Additionally, the Commission should conduct an annual review of its IT Risk Management and Contingency Planning documents to ensure they reflect the Commission's current environment and distribute the updated versions to key staff. Taking these corrective actions will help ensure the confidentiality, integrity, and availability of sensitive and mission essential systems and business functions.

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

The Commission has made progress in performing pre-implementing testing of system changes, remediating one of the two weaknesses in the prior year finding. However, the Commission continues not to consistently perform an evaluation of change requests from a security perspective, commonly referred to as a security impact analysis, in accordance with its Configuration Management Policy and Procedure and the Security Standard.

The Commission's Configuration Management Policy and Procedure requires the Commission's Information Security Officer (ISO), or designee within the Commission's Information Security Division, to perform a security impact analysis for proposed changes to its systems and applications, document the findings, and attach the document to the change request. Additionally, the Security Standard requires the Commission to approve or deny change requests with an explicit consideration of the security impact

analysis. Without conducting and documenting a security impact analysis for each requested change, the Commission may not detect and prevent changes that could compromise the security of its IT environment.

While the Commission implemented the process to conduct a security impact analysis for system change requests in accordance with its Configuration Management Policy and Procedure, the Commission's Change Advisory Board found it needed additional guidelines from the ISO to consistently determine when a change requires a security impact analysis. For certain changes during the fiscal year, this led to staff not notifying the ISO that a security impact analysis was needed or inaccurately documenting that one was not needed.

The Commission should continue the implementation of its process and ensure that it conducts security impact analyses for changes in accordance with its Configuration Management Policy and Procedure and the Security Standard. If the Commission determines it does not need to conduct a security impact analysis for a change, it should document this determination for the change request. Improving the change control process will help ensure the confidentiality, integrity, and availability of sensitive and mission critical data.

Document Database Audit Logging and Monitoring Procedures

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2024

In our prior report, we identified that the Commission did not have a formal documented policy, nor procedures related to the audit logging and monitoring for its databases. The Security Standard requires the Commission to develop, document, and disseminate an audit and accountability policy and procedure to facilitate the implementation of audit and accountability controls. Management does not expect to complete corrective actions to remediate the prior year finding until fiscal year 2026. As management plans to complete corrective action after the fiscal year under review, we will evaluate whether the corrective actions achieved the desired results during the fiscal year 2026 audit.

Improve Vulnerability Management

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2024

In our prior report, we identified that the Commission did not remediate vulnerabilities classified with a severity of medium or low within the timeframe required by the Security Standard and the Commonwealth's IT Risk Management Standard, SEC520. Management does not expect to complete corrective actions to remediate the prior year finding until fiscal year 2026. As management plans to complete corrective action after the fiscal year under review, we will evaluate whether the corrective actions achieved the desired results during the fiscal year 2026 audit.

Strengthen Interdepartmental Communications Related to Terminated Employees
Type: Internal Control and Compliance
Severity: Significant Deficiency

The Commission does not have adequate internal controls for disabling access to the internal benefits system for terminated employees. In our review of 20 employees with system access who terminated during the fiscal year, we identified five (25%) instances in which the supervisor requested access be disabled between two and fifteen days after the employee's termination from the Commission. In all five instances, the timing of supervisor's request resulted in untimely disabling of access to the Commission's internal benefits system.

The Commission's Access Control Policy and the Security Standard require an employee's system access to be disabled within 24 hours of termination. Untimely deletion of access to sensitive systems increases the risk of unauthorized transactions and access to sensitive data by individuals no longer employed by the Commission. Disabling of a terminated employee's access to the system by the system manager is dependent on submission of termination details by the supervisor or another knowledgeable party such as Human Resources. Our review determined that the system manager removes access timely upon receipt of separation notification.

The Commission should strengthen communication between supervisors, Human Resources, and the systems manager to ensure timely disabling of system access. Management should develop and formalize procedures for offboarding employees and communicate to supervisory staff the importance of these procedures to ensure supervisors notify appropriate parties of an employee's separation in a timely manner.

Document Annual System Access Reviews
Type: Internal Control and Compliance
Severity: Significant Deficiency

Management of the Commission did not document their annual review of access to the Commission's internal benefits system for the period under audit. While management asserts that they conducted a review, they did not create and retain documentation of their review.

The Commission's Access Control Policy and the Security Standard require the agency to review accounts for compliance with account management requirements on an annual basis. Within the broader context of the Security Standard, it suggests that activities supporting compliance must be documented. For example, service providers are required to document their account management practices. Not documenting activities supporting compliance prevents executive leadership from reviewing and validating that employees are performing the tasks required to reduce the risk of individuals having unnecessary system access.

While the Commission has its Access Control Policy, it does not include an explicit requirement for managers to create and retain documentation of their annual system access reviews, nor has it developed formalized procedures for documenting system access reviews. The Commission should

formalize procedures governing the account management of access to the internal benefits system which will assist in ensuring the proper completion and documentation of annual access reviews. Furthermore, management should document their completion of the required annual review of access to the Commission's internal benefits system.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 12, 2025

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

George "Bryan" Slater
Secretary of Labor

Demetrios Melis
Commissioner, Virginia Employment Commission

We have audited the financial records and operations of the **Virginia Employment Commission** (Commission) 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 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 the Commission's financial transactions as reported in the Annual Comprehensive Financial Report for the Commonwealth of Virginia 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, the Commission's accounting and financial reporting system, the Commission's benefits and tax, and financial systems, and the enterprise fund template submitted to the Department of Accounts (Accounts); reviewed the adequacy of the Commission'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

The Commission'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 significant cycles, classes of transactions, and account balances:

Unemployment Compensation, a major enterprise fund in the Annual Comprehensive Financial Report for the Commonwealth of Virginia:

- Cash with the U.S. Department of the Treasury, Unemployment Trust
- Benefit eligibility determination and payment
- Revenue collections, reimbursement for services and taxes
- Receivables, due from: claimants (including penalties), employers, and other states
- Due to benefit claimants, employers, and other governments

Commonwealth's retirement benefits system

Information system security and general system controls (including access controls)

The scope of our audit did not include the significant cycles, classes of transactions, or account balances of the Department of Workforce Development and Advancement (Virginia Works), or shared services that the Commission provides to Virginia Works. Accordingly, this report does not include such information.

We performed audit tests to determine whether the Commission'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 the Commission's operations. We performed analytical procedures, including budgetary and trend analyses, and tested details of transactions to achieve our audit objectives. We also confirmed cash with the federal government.

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. However, as described in the section titled "Internal Control and Compliance Findings and Recommendations," we identified certain deficiencies in internal control that we consider to be material weaknesses and significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. We consider the deficiency titled "Improve Internal Controls over the Collection and Reporting of Accounts Receivable," 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 deficiencies titled "Allocate and Align Resources to Reduce IT Security Risk," "Improve IT Risk Management and Contingency Planning Program," "Improve Change Control Process," "Document Database Audit Logging and Monitoring Procedures," "Improve Vulnerability Management," "Strengthen Interdepartmental Communications Related to Terminated Employees," and "Document Annual System Access Reviews," which are described in the section titled "Internal Control and Compliance Findings and Recommendations," to be significant deficiencies.

Conclusions

We found that the Commission properly stated, in all material respects, the amounts recorded and reported in the Commonwealth's accounting and financial reporting system, the Commission's benefits and tax, and financial systems, and the enterprise fund template submitted to Accounts after adjustment for the misstatements noted in the finding "Improve Internal Controls over the Collection and Reporting of Accounts Receivable."

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."

The Commission has taken adequate corrective action with respect to the prior audit finding 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 or significant deficiencies, they will be reported as such in the "Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of the

Financial Statements Performed in Accordance with Government Auditing Standards," which is 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 February 3, 2026. Government Auditing Standards require the auditor to perform limited procedures on the Commission's response to the findings identified in our audit, which is included in the accompanying section titled "Agency Response." The Commission'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

GDS/clj

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	Fiscal Year First Reported
Improve Security Awareness Training Program	Complete	2024
Improve Internal Controls over the Collection and Reporting of Accounts Receivable	Ongoing	2025
Allocate and Align Resources to Reduce IT Security Risk	Ongoing	2025
Improve IT Risk Management and Contingency Planning Program	Ongoing	2024
Improve Change Control Process	Ongoing	2023
Document Database Audit Logging and Monitoring Procedures	Ongoing	2024
Improve Vulnerability Management	Ongoing	2024
Strengthen Interdepartmental Communications Related to Terminated Employees	Ongoing	2025
Document Annual System Access Reviews	Ongoing	2025

* 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.

COMMONWEALTH of VIRGINIA
Virginia Employment Commission

Melissa Smith
Commissioner

Post Office Box 26441
Richmond, VA 23261-6441

February 3, 2026

Ms. Staci Henshaw
Auditor of Public Accounts
Post Office Box 1295
Richmond, Virginia 23218

Dear Ms. Henshaw:

Thank you for the opportunity to review and respond to your Audit Report of the Virginia Employment Commission (VEC) covering the fiscal year ended June 30, 2025. We will work diligently to implement appropriate corrective actions to address the audit findings.

The VEC remains steadfast in its commitment to strengthening internal controls, enhancing information security, and maintaining full compliance, while advancing our mission to provide seamless, innovative, and timely services to the citizens of the Commonwealth of Virginia.

Please let me know if you have any questions.

Sincerely,

Melissa Smith

(804) 786-3001
www.vec.virginia.gov