VIRGINIA EMPLOYMENT COMMISSION

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 Virginia Employment Commission (Commission) 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 reporting system, the Commission's benefits and tax, and financial systems, and the enterprise fund template submitted to the Department of Accounts (Accounts);

- five 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

- corrective action on prior audit finding remains ongoing as indicated 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 audits 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 IT Risk Management and Contingency Planning Program
Type: Internal Control and Compliance
Severity: Significant Deficiency

The Virginia Employment Commission (Commission) does not ensure appropriate collaboration for the development and maintenance of its information technology (IT) risk management and contingency planning program. As a result, the Commission does not conduct and maintain its IT risk management and contingency planning documents in accordance with the Commonwealth's IT Security Standard, SEC530 (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). Specifically, the following weaknesses exist:

- The Commission does not use information documented in the BIA as the primary input to its other IT risk management and contingency planning documents. The BIA delineates the steps necessary for organizations to identify the business functions that are essential to the organization's mission and the resources required to support the essential functions. The Security Standard requires the Commission to use the IT information documented in the BIA as a primary input to Sensitivity Classifications, RAs, COOP, and SSPs. As a result, the Commission does not consistently define essential information between its BIA and COOP, including:

    - Mission essential functions (MEF)
    - Primary business functions (PBF)
    - IT systems and resources that support each MEF and PBF
    - Recovery Time Objectives
    - Recovery Point Objectives

    The inconsistent information across its IT risk management and contingency planning documents may delay the Commission recovering its MEFs and supporting IT systems in the event of a disruption or disaster.

- The Commission does not include certain IT risk management requirements within its Contingency Planning Policy and Procedures or Risk Assessment Policy and Procedures as required by the Security Standard. Specifically, the Commission does not include requirements for how it will conduct a BIA and use it as the primary input to its Sensitivity Classifications, RA, COOP and SSPs. Additionally, the Commission does not define requirements to conduct SSPs and Sensitivity Classifications based on confidentiality, integrity, and availability. By not ensuring its policies 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 and document annual reviews for some of its IT risk management and contingency planning documents in accordance with the Security Standard to validate the information is 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. Specifically, the Commission does not review and update the following documents:

    - Sensitive Systems List
    - IT Disaster Recovery Plan
    - IT Hardware and Software Assets List

- The Commission does not conduct an RA for each of its 16 known sensitive systems. The Security Standard requires the Commission to conduct and document an RA for each system classified as sensitive as needed, but not less than once every three years. Without current and complete risk assessments, 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 the system and data.

- The Commission has not developed a SSP for one of its known sensitive systems and does not include certain elements for the other 15 SSPs, as required by the Security Standard. 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 security and privacy related activities affecting the system that require planning and coordination with organization defined individuals or groups.

- The Commission did not determine and include contingency procedures for one of its three MEFs within its COOP. The Security Standard requires the Commission to identify essential mission and business functions and associated contingency requirements. Additionally, the Security Standard requires the Commission to address maintaining essential missions and business functions despite an information system disruption, compromise, or failure. By not defining contingency procedures or identifying the resources required to enable the contingency procedures, the Commission's staff may be unprepared and ill-equipped to maintain MEFs and PBFs in the event of a disaster.

- The Commission does not perform an annual test of its COOP and does not document lessons learned from the annual exercise of its DRP to facilitate updates to the plan and supporting procedures. The Security Standard requires the Commission to conduct annual exercises to

test the COOP and DRP to determine effectiveness and readiness to execute the plan. The Security Standard requires the Commission to update the contingency plan to address problems encountered during contingency plan implementation, execution, or testing.

- The Commission did not provide evidence that it protects contingency planning documentation from unauthorized disclosure or modification as required by the Security Standard. Without protecting contingency planning documentation from unauthorized disclosure or modification, the Commission increases the risk of unauthorized changes and inaccurate incident response procedures in its COOP and DRP.

- The Commission does not appropriately distribute updated versions of its continuity plan to executive leadership and key personnel as required by the Security Standard. Without communicating contingency plans to key personnel, the Commission increases the risk of inconsistent contingency responses that could result in delayed response and misaligned actions.

Without appropriate collaboration amongst the necessary business and IT divisions, the Commission cannot know if its IT risk management and contingency planning documents encompass all the necessary and accurate information. Additionally, without completing, maintaining, testing, protecting, and communicating the IT risk management and contingency planning documents, the Commission increases the risk for ineffective incident response, operational disruption, and data loss.

During fiscal year 2024, the Commission assisted in developing the new Virginia Works Agency, which resulted in resource constraints for all departments within the Commission. As the new agency has been established, the Commission should dedicate resources necessary to improve its policies, procedures, and collaboration to ensure it uses the BIA as a primary input for its other IT risk management and contingency planning documents and that each document aligns with the requirements of the Security Standard. The Commission should also ensure it identifies and documents contingency procedures for its MEFs and PBFs, conduct annual tests of its COOP and DRP to determine the effectiveness of the procedures, and document the lessons learned. Additionally, the Commission should conduct annual reviews of its IT Risk Management and Contingency Planning policies and documents to make updates as necessary to reflect the Commission's current environment and distribute the updated versions to key staff. Improving its IT risk management and contingency planning program will help the Commission 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 since the prior year audit to revise its Configuration Management Policy and Procedure (Configuration Policy) to define whether certain types of changes are exempt from certain elements of the Security Standard IT change control requirements. However, the Commission continues to not consistently follow its Configuration Policy, which is based on the Security Standard. Specifically, the Commission continues not to perform the following:

- The Commission does not consistently perform an explicit evaluation of change requests from a security perspective, commonly referred to as a security impact analysis, for changes to its systems and applications. The Configuration Policy 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 explicit consideration for security impact analyses. 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 the IT environment.

- The Commission did not provide documentation for all 25 sampled changes to indicate if it performed pre-implementation testing. The Security Standard requires the Commission's personnel with security or privacy responsibilities, as set by its Configuration Policy, to test, validate, and document changes to the information system before implementing the changes on the operational system. Without performing pre-implementation testing to validate a change, the Commission increases the risk that a change that may compromise security of the IT environment will not be detected and prevented.

While the Commission revised its Configuration Policy in April 2024 based on the Security Standard, it delayed implementing the new process due to the Commission dedicating staff to assist with the establishment of the new Virginia Works Agency. As the new agency has been established, the Commission should dedicate the resources necessary to ensure that it conducts security impact analyses and pre-implementation testing for changes in accordance with its Configuration Policy and the Security Standard. Improving the change control process will help the Commission 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

The Commission does not have a formal documented policy nor procedures for audit logging and monitoring a sensitive database that is mission critical. 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.

The Commission uses its database to process significant transactions and contains protected personally identifiable information, making it imperative for the Commission to log and monitor database activity. Without developing and documenting formal monitoring procedures for this database, VEC increases the risk that the Commission will not properly monitor audit logs, which could result in a lack of accountability, data integrity issues, and inefficient incident response. Specifically, the Commission cannot verify that it has implemented audit logging and monitoring controls that include, but are not limited to:

- Identifying the types of audit events that the Commission should log and monitor;
- Reviewing and analyzing audit records for unusual activity and reporting findings to the necessary officials;
- Protecting audit information from unauthorized access, modification, and deletion; and
- Enforcing separation of duties for monitoring administrative activity.

During fiscal year 2024, the Commission assisted in developing the new Virginia Works Agency, which resulted in significant resource constraints for all departments within the Commission. As the new agency has been established, the Commission should dedicate the resources necessary to develop and document a formal audit logging and monitoring policy that aligns with the Security Standard's minimum requirements and delineates the Commission's expectations. The Commission should then develop and document formal procedures that outline the Commission's processes for meeting the requirements detailed in its policy. These corrective actions will help the Commission ensure the confidentiality, integrity, and availability of sensitive and mission critical data.

Improve Vulnerability Management

Type: Internal Control and Compliance

Severity: Significant Deficiency

The Commission currently has numerous vulnerabilities classified with a severity of medium or low, which the Commission has not remediated within the required timeframe. Collectively, the Security Standard, and the Commonwealth's IT Risk Management Standard, SEC520 (Risk Management Standard) require the Commission to identify and remediate risks in a timely manner. Specifically, the Security Standard requires the Commission to "monitor and scan for vulnerabilities in the system and hosted

applications at least once every 30 days, and when new vulnerabilities potentially affecting the system are identified and reported." Additionally, the Security Standard requires the Commission to remediate legitimate vulnerabilities within 30 days unless otherwise specified by the Commonwealth Security Risk Management (CSRM) division in accordance with an organizational assessment of risk. The Risk Management Standard requires the Commission to "fix vulnerabilities within 30 days of a fix becoming available that are either rated as critical or high (Common Vulnerability Scoring System v3 score of 7-10) according to the National Vulnerability Database or otherwise identified by CSRM." Additionally, the Risk Management Standard requires the Commission to remediate all other vulnerabilities within 90 days of a fix becoming available and acquire an approved security exception for the vulnerability should the Commission not remediate it within the timeframes identified.

Software vulnerabilities are publicly known flaws that bad actors may exploit and use to circumvent organizational information security controls to infiltrate a network or application. The longer these vulnerabilities exist in an environment, the higher the risk of compromise and unauthorized access to sensitive and mission-critical systems and data. It is therefore imperative for organizations to respond quickly and mitigate these publicly known flaws as soon as possible. Without appropriate software patching and vulnerability management controls, the Commission increases the risk of unauthorized access to sensitive and mission-critical systems.

These un-remediated risks exist because during fiscal year 2024, the Commission assisted in developing the new Virginia Works Agency, which resulted in significant resource constraints for all departments within the Commission. Furthermore, the Commission does not have a formal policy and process to determine and document whether a vulnerability is the responsibility of the Commission or contractors procured by Virginia Information Technologies Agency (VITA). As a result, the Commission does not remediate vulnerabilities affecting its IT environment as required.

The Commission should develop and implement a process to determine and document whether vulnerabilities are the responsibility of VITA contractors or the Commission to remediate. For vulnerabilities that fall under the responsibility of VITA's external contractors, the Commission should communicate with VITA any outstanding vulnerabilities to ensure remediation. For those under the Commission's responsibility, the Commission should mitigate the legitimate vulnerabilities within the timeframe required by the Security Standard and Risk Management Standard. If the Commission is unable to mitigate vulnerabilities within the required timeframe, it should seek an extension approval from VITA's CSRM division that is based on an organization assessment of risk. Timely remediation of significant vulnerabilities will help protect the confidentiality, integrity, and availability of the Commission's sensitive and mission critical data.

Improve Security Awareness Training Program

Type: Internal Control and Compliance

Severity: Significant Deficiency

The Commission 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 Commonwealth's Security Standard, and the Commonwealth's Security Awareness Training

Standard, SEC527 (Training Standard). The Security Standard makes the Commission's ISO responsible for developing and maintaining a SAT program, which is essential to ensuring that users understand their roles and responsibilities in securing sensitive information of the Commission. However, the Commission is not complying as follows:

- The Commission's ISO does not provide SAT to employees when they are first employed. The Training Policy, which is based on the Security Standard, requires the Commission's ISO to provide security and privacy literacy training to new system users and annually thereafter. The Training Standard requires the Commission's ISO to ensure all IT system users complete IT security awareness and training activities within 30 days of initial access and by January 31st each year thereafter. Without providing security awareness training to individuals upon their initial system access, the Commission increases the risk that new users will not identify and respond to security threats that could compromise sensitive systems and data.

- The Commission's ISO does not monitor and enforce compliance to ensure each user completes the required training. As a result, five out of 489 (1%) users did not have training accounts created to complete the SAT, and another 41 (8.3%) employees did not complete the Commission's most recent annual SAT. The Training Policy requires the Commission's ISO to provide basic SAT to information system users as part of initial training for new users and annually or more often as necessary thereafter. The Training Standard requires the Commission's ISO to ensure all IT system users complete IT security awareness and training activities within 30 days of initial access and by January 31st each year thereafter. Without a process to monitor and enforce users to complete training, such as disabling a user's access, the Commission increases the risk that employees will be more susceptible to malicious attempts to compromise sensitive data, such as ransomware, phishing, and social engineering.

During fiscal year 2024, the Commission assisted in developing the new Virginia Works Agency, which resulted in resource constraints for all departments within the Commission. Additionally, the Commission's ISO was not aware of the requirement to retain evidence of processes for administering and monitoring training to ensure compliance with the Training Policy and the related standards. The Commission's ISO should ensure new users complete SAT within 30 days of their initial access. The Commission's ISO should also improve its process to monitor and enforce all users in completing their annual SAT as required by the Training Policy, Security Standard, and Training Standard. These corrective actions will help protect the Commission from malicious attempts to compromise the confidentiality, integrity, and availability of sensitive and mission critical data.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 13, 2024

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

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, 2024. We conducted this audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, in support of the Commonwealth's Annual Comprehensive Financial Report audit. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Objectives

Our audit's primary objective was to evaluate the accuracy of the Commission's financial transactions as reported in the Annual Comprehensive Financial Report for the Commonwealth of Virginia for the year ended June 30, 2024. In support of this objective, we evaluated the accuracy of recorded financial transactions in the Commonwealth's accounting and financial reporting system, 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 action with respect to the audit finding and recommendation from the prior year report.

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 to employers and other governments

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

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. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control titled "Improve IT Risk Management and Contingency Planning Program," "Improve Change Control Process," "Document Database Audit Logging and Monitoring Procedures," "Improve Vulnerability Management," 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 on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Conclusions

We found that 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 enterprise fund template 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."

Since the findings noted above include those that have been identified as significant deficiencies, they will be reported as such in the "Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of the Financial Statements Performed in Accordance with Government Auditing Standards," which is included in the Commonwealth of Virginia's Single Audit Report for the year ended June 30, 2024. The Single Audit Report will be available at www.apa.virginia.gov in February 2025.

Exit Conference and Report Distribution

We provided management of the Commission with a draft of this report on January 28, 2025, for review. 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*	First Reported for Fiscal Year
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
Improve Security Awareness Training Program	Ongoing	2024

* 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

Demetrios J. Melis
Commissioner

Post Office Box 2644
Richmond, VA 23261-644

February 5, 2025

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) for the fiscal year ended June 30, 2024.

We concur with the audit findings and your recommendations are given the highest level of importance and consideration as we navigate the necessary steps to resolve the audit concerns.

The VEC remains committed to strengthening our internal controls and compliance while furthering our goal to deliver seamless, innovative and timely services to the citizens of the Commonwealth of Virginia.

Please let me know if you have any questions.

Sincerely,

Demetrios Melis

(866) 832-2363
E-Mail: CustomerService@vec.virginia.gov