



# VIRGINIA ECONOMIC DEVELOPMENT PARTNERSHIP

## REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2023

Auditor of Public Accounts  
Staci A. Henshaw, CPA

[www.apa.virginia.gov](http://www.apa.virginia.gov)

(804) 225-3350



## AUDIT SUMMARY

We have audited the basic financial statements of the Virginia Economic Development Partnership (Partnership) as of and for the year ended June 30, 2023, and issued our report thereon, dated June 3, 2024. Our report, included in the Partnership's Annual Report, is available at the Auditor of Public Accounts' website at [www.apa.virginia.gov](http://www.apa.virginia.gov) and at the Partnership's website at [www.vedp.org](http://www.vedp.org). Our audit of the Partnership found:

- the financial statements are presented fairly, in all material respects;
- two internal control findings, first issued for fiscal year 2022, requiring management's continued attention that also represent instances of noncompliance or other matters required to be reported under Government Auditing Standards; however, we do not consider them to be material weaknesses. The [Findings Summary](#) included in the Appendix identifies the status of corrective action on these prior findings as ongoing.

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 the Department of Accounts in Section 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendations.

## –TABLE OF CONTENTS–

### Pages

AUDIT SUMMARY

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

1-2

INDEPENDENT AUDITOR’S REPORT ON INTERNAL CONTROL OVER  
FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

3-5

APPENDIX – FINDINGS SUMMARY

6

PARTNERSHIP RESPONSE

7

## INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

### **Improve Information Security Program and IT Governance**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**First Issued:** Fiscal Year 2022

The Partnership has made significant improvements to its information security program and information technology (IT) governance structure by following its established roadmap to address the issues identified during our last audit. However, as it takes time to implement controls to address the issues, the Partnership has not yet finished implementing all corrective actions and some remain outstanding. We communicated four control 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 its sensitivity and description of security controls.

The Partnership's adopted security standard, the Commonwealth's Information Security Standard, SEC 530 (Security Standard), Section 2.4.2, requires the agency head to maintain an information security program that is sufficient to protect the agency's IT systems and to ensure the agency documents and effectively communicates its information security program.

Not having a comprehensive and updated IT governance structure to properly manage the Partnership's IT environment and information security program can create weaknesses that result in a data breach or unauthorized access to confidential and mission critical data, leading to data corruption, data loss, or system disruption if accessed by a malicious attacker, either internal or external. The control weaknesses described above are the result of the Partnership focusing remediation efforts on establishing a comprehensive roadmap to improve its information security program. The lengthy timeline required to complete all remediation efforts also contributed to ongoing weaknesses.

The Partnership should complete its remediation plan to bring its IT security program in compliance with the Security Standard. Specifically, the Partnership should implement the planned IT governance changes to address the control deficiencies discussed in the communication marked FOIAE. Implementing these recommendations will help to ensure the Partnership protects the confidentiality, integrity, and availability of its sensitive and mission critical data.

### **Improve Service Provider Oversight**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**First Issued:** Fiscal Year 2022

The Partnership has made progress since our last audit, but needs to continue to strengthen policies, procedures, and processes to manage risks from the use of external information system services, including monitoring the effectiveness of security controls of external service providers. Service providers are organizations that perform certain business tasks or functions on behalf of the Partnership

and the Commonwealth. The Partnership uses 28 service providers for business functions that include the processing and storing of sensitive data.

The Security Standard states management remains accountable for maintaining compliance with the Security Standard through documented agreements with service providers and oversight of services provided (*Section 1.1-Intent*). Additionally, the Security Standard requires that organizations document a system and services acquisition policy, as well as procedures to facilitate the implementation of the policy and associated controls (*SA-1 System and Services Acquisition Policy and Procedures*). The Security Standard states that organizations must ensure that providers of external information system services comply with the organization's security requirements and employ appropriate security controls. The Security Standard further requires that organizations must define and document roles and responsibilities regarding external information system services. Finally, the Security Standard requires that organizations define and employ processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis (*SA-9 External Information System Services*).

By not defining, documenting, and employing a process to gain continuous assurance over service providers' operating controls, the Partnership cannot validate that the service providers have effective security controls to protect the Partnership's sensitive and confidential data. The Partnership engaged a contractor and in July 2023, completed a roadmap to improve its information security program that includes plans to document and approve formalized information security policies, procedures, standards, and guidelines. However, the Partnership has not yet completed the planned policies, procedures, and processes for maintaining oversight over service providers, which impacted the Partnership gaining assurance over outsourced operations. The Partnership also obtained independent audit assurance reports from 18 of the 28 service providers but has not completed a formal review and evaluation of the 18 reports due to the lack of a procedure detailing the review process.

The Partnership should complete, approve, and implement the planned policies, procedures, and processes to monitor the effectiveness of security controls of external service providers. The Partnership should then communicate the required security controls, as well as the roles and responsibilities of each party, through documented agreements with its service providers. Additionally, the Partnership should obtain independent audit assurance reports from the ten remaining service providers and evaluate the independent audit assurance reports received from each to ensure the service provider has effective operating controls to protect the Partnership's sensitive and mission critical data. During the evaluation, the Partnership should identify control deficiencies, develop mitigation plans, escalate issues of noncompliance, and implement complementary user entity controls, as needed. Finally, the Partnership should document its evaluation of independent audit assurance reports. Gaining sufficient assurance over each service provider's security controls will help to ensure the confidentiality, integrity, and availability of sensitive and mission critical data.



Staci A. Henshaw, CPA  
Auditor of Public Accounts

# Commonwealth of Virginia

*Auditor of Public Accounts*

P.O. Box 1295  
Richmond, Virginia 23218

June 3, 2024

The Honorable Glenn Youngkin  
Governor of Virginia

Joint Legislative Audit  
and Review Commission

Board of Directors  
Virginia Economic Development Partnership

Jason El Koubi, President and CEO  
Virginia Economic Development Partnership

## **INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS**

We have audited, in accordance with the 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, the financial statements of the governmental activities and each major fund of the **Virginia Economic Development Partnership** (Partnership) as of and for the year ended June 30, 2023, and the related notes to the financial statements, which collectively comprise the Partnership's basic financial statements, and have issued our report thereon dated June 3, 2024.

### **Report on Internal Control Over Financial Reporting**

In planning and performing our audit of the financial statements, we considered the Partnership's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Partnership's internal control. Accordingly, we do not express an opinion on the effectiveness of the Partnership's internal control.

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.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section 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 Information Security Program and IT Governance" and "Improve Service Provider Oversight" which are described in the section titled "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies.

### **Compliance and Other Matters**

As part of obtaining reasonable assurance about whether the Partnership's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements noncompliance with which could have a direct and material effect on the financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under Government Auditing Standards and which are described in the section titled "Internal Control and Compliance Findings and Recommendations" in the findings and recommendations titled "Improve Information Security Program and IT Governance" and "Improve Service Provider Oversight."

### **The Partnership's Response to Findings**

We discussed this report with management at an exit conference held on May 21, 2024. Government Auditing Standards require the auditor to perform limited procedures on the Partnership's response to the findings identified in our audit, which is included in the accompanying section titled "Partnership Response." The Partnership's response was not subjected to the other auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the response.

### **Status of Prior Findings**

The Partnership has not completed adequate corrective action with respect to the prior reported findings and recommendations identified as ongoing in the [Findings Summary](#) included in the Appendix.

### **Purpose of this Report**

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with Government Auditing Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Staci A. Henshaw  
AUDITOR OF PUBLIC ACCOUNTS

LCW/clj



## FINDINGS SUMMARY

Finding Title	Status of Corrective Action	First Issued
Improve Information Security Program and IT Governance	Ongoing	2022
Improve Service Provider Oversight	Ongoing	2022

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

Ms. Staci A. Henshaw  
Auditor of Public Accounts  
James Monroe Building  
101 N. 14th Street  
Richmond, Virginia 23219

Dear Ms. Henshaw:

The Virginia Economic Development Partnership (VEDP) has reviewed the findings and recommendations provided by the Auditor of Public Accounts as part of your audit of VEDP's financial records for the year ended June 30, 2023. VEDP appreciates the opportunity to respond to the Internal Control and Compliance Findings and Recommendations included in your report, and we give your comments the highest level of consideration.

**Internal Control and Compliance Findings and Recommendations**

**Improve Information Security Program and IT Governance**

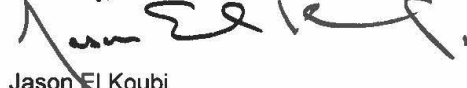
VEDP has made significant improvements to our information security program and IT governance structure and is working diligently with our security partner on the roadmap to achieve full compliance with SEC530. Substantial completion of the roadmap is expected by December 2024, and we look forward to sharing our continued progress at the next audit. VEDP is aligning risk management and contingency planning efforts for each department alongside formal data classifications and risk assessments this summer. The output of these assessments will feed VEDP's ongoing continuity and disaster recovery planning efforts.

VEDP has developed a five-year audit plan to audit sensitive systems every three years and is approaching completion of two sensitive system audits. We are underway with formal evaluation of independent audit assurance reports using the new Vendor Risk Analysis form. VEDP Information Technology and Fiscal & Support divisions will work together with our accounting system partner and Virginia Tourism Corporation (VTC) to transfer from the end-of-life Great Plains by October 2024, ensuring fully supported systems across VEDP and VTC.

**Improve Service Provider Oversight**

VEDP has made significant efforts to improve service provider oversight and is working diligently to formalize the procurement and evaluation of these service providers. VEDP has nearly completed two sensitive system audits and is now utilizing our Vendor Risk Analysis form and processes to evaluate independent audit assurance reports. We hope to share our continued progress at the next audit.

Sincerely,



Jason El Koubi  
President and CEO