DEPARTMENT OF THE TREASURY

REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2024

Auditor of Public Accounts
Staci A. Henshaw, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

Our audit of the Department of the Treasury (Treasury) 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, Treasury's internal accounting and reporting systems, and supplemental information and attachments submitted to the Department of Accounts;

- one matter involving internal control and its operation necessary to bring to management's attention that also represents an instance of noncompliance with applicable laws and regulations or other matters that is required to be reported; and

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

In the section titled "Internal Control and Compliance Finding and Recommendation," we have included our assessment of the conditions and causes resulting in the internal control and compliance finding identified through our audit as well as recommendations for addressing the finding. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the finding and develop and appropriately implement adequate corrective actions to resolve the finding as required by the Department of 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.

Additionally, our report includes one risk alert that requires the action and cooperation of Treasury management and the Virginia Information Technologies Agency (VITA) regarding risks related to access to centralized audit log information.

In fiscal year 2023, we included the results of our audit over Treasury in the report titled Agencies of the Secretary of Finance for the year ended June 30, 2023.

-TABLE OF CONTENTS-

INTERNAL CONTROL AND COMPLIANCE FINDING AND RECOMMENDATION

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

Treasury does not remediate vulnerabilities affecting a web application in accordance with the Commonwealth's Information Security Standard, SEC530 (Security Standard), and the Commonwealth's Information Technology (IT) Risk Management Standard, SEC520 (Risk Management Standard). Specifically, Treasury did not remediate three vulnerabilities it detected in its vulnerability scans starting in August 2023. Additionally, Treasury did not update its Threat Management Policy to align with the current requirements of the Security Standard, as it continues to reflect outdated requirements for installing security patches to mitigate vulnerabilities.

The Security Standard requires Treasury 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 Treasury to remediate legitimate vulnerabilities within 30 days unless otherwise specified by Commonwealth Security Risk Management (CSRM) in accordance with an organizational assessment of risk. The Risk Management Standard requires Treasury to "fix vulnerabilities within 30 days of a fix becoming available that are either rated as critical or high (CVSS V3 Score of 7-10) according to the National Vulnerability Database (NVD) or otherwise identified by CSRM." Additionally, the Risk Management Standard requires Treasury to remediate all other vulnerabilities within 90 days of a fix becoming available and acquire an approved security exception for the vulnerability should Treasury 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 vulnerabilities as soon as possible. Without appropriate software patching and vulnerability management controls, Treasury increases the risk of unauthorized access to sensitive and mission-critical systems.

Treasury did not remediate the vulnerabilities affecting the web application because it prioritized mitigating vulnerabilities affecting other web applications that posed a greater risk to the agency's IT environment with plans to address internal applications in the fall of 2024. Additionally, while Treasury updated its Threat Management Policy in August 2024, Treasury did not update the required timeframe for applying patches to mitigate vulnerabilities due to an oversight during the revision process.

Treasury should review and revise its Threat Management Policy to ensure its vulnerability management process aligns with the requirements outlined in the Security Standard. Treasury should then implement its process to mitigate legitimate vulnerabilities affecting its IT environment within the

timeframe required by its Threat Management Policy and the Security Standard. If Treasury is unable to mitigate vulnerabilities within the required timeframe, it should request an extension approval from CSRM that is based on an organizational assessment of risk. Timely remediation of significant vulnerabilities will help protect the confidentiality, integrity, and availability of Treasury's sensitive and mission-critical information.

RISK ALERTS

During our audit, we encountered an issue that is beyond the corrective action of Treasury's management alone and requires the action and cooperation of management and the Virginia Information Technologies Agency (VITA). The following issue represents such a risk to Treasury and the Commonwealth.

Access to Centralized Audit Log Information

Treasury relies on the Commonwealth's Information Technology Infrastructure Services Program (ITISP) to install, maintain, operate, and support IT infrastructure components, such as servers, routers, firewalls, and virtual private networks. As part of these services, Treasury relies on contractors procured by VITA to provide Treasury access to a centralized monitoring tool, known as the Managed, Detection, Response (MDR) Dashboard, that collects audit log information about activities in Treasury's IT environment so that Treasury can review logged activity. Additionally, Treasury relies on VITA to maintain oversight and enforce the service level agreements and deliverables with the ITISP contractors.

While VITA did not originally enforce the deliverable requirement when ratifying the ITISP contracts in 2018, VITA tried to compel the ITISP contractor to grant agencies, such as Treasury, access to the monitoring tool and audit log information for the last five years. The MDR Dashboard went live in October 2023 but did not include all audit log information to allow agencies to adequately monitor their IT environments. Additionally, VITA implemented a separate security and event management (SIEM) tool at the end of October 2023 to expand agencies' capabilities to monitor audit log information. As of October 2024, VITA and the ITISP supplier determined the MDR Dashboard will be replaced by the VITA-managed SIEM tool as the permanent audit log monitoring tool. However, while the VITA-managed SIEM tool is in production, it also does not include all audit log information in a usable format to allow agencies to adequately monitor their IT environments.

The Security Standard requires a review and analysis of audit records at least every 30 days for indications of inappropriate or unusual activity and assessment of the potential impact of the inappropriate or unusual activity. Using a SIEM tool without all necessary audit log information reduces organizational security posture by not being able to react to and investigate suspicious system activity in a timely manner. Treasury is working with VITA to import audit log information to the SIEM tool and provide feedback on its uses to ensure Treasury can review the activities occurring in its IT environment in accordance with the Security Standard. 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

December 13, 2024

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Stephen E. Cummings
Secretary of Finance

David L. Richardson
State Treasurer

We have audited the financial records and operations of the **Department of the Treasury** (Treasury) 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 financial transactions related to cash and cash equivalents, investments, debt, unclaimed property, and risk management originating at Treasury, 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, Treasury's internal accounting and reporting systems, and supplemental information and attachments submitted to the Department of Accounts; reviewed the adequacy of Treasury's internal control; tested for compliance with applicable laws, regulations, contracts, and grant agreements; and reviewed corrective actions with respect to audit findings and recommendations from prior year reports.

Audit Scope and Methodology

Treasury'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 processes and systems.

- Financial reporting*
- Cash management and banking
- Bank reconciliation system
- Bond issuance
- Debt servicing
- Information security and general system controls (including access controls)
- Investment trading
- Investment accounting
- Investment accounting systems
- Trust accounting
- Management of unclaimed property
- Risk management claim processing

*Including preparation of financial statements of the Local Government Investment Pool Program, the Virginia College Building Authority, the Virginia Public Building Authority, and the Virginia Public School Authority.

We performed audit tests to determine whether Treasury'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 Treasury's operations. We performed analytical procedures, including budgetary and trend analyses, and tested details of transactions to achieve our audit objectives. We also confirmed bank and investment account balances and literary loan receivables with outside parties.

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 a deficiency in internal control titled "Improve Vulnerability Management

Process" which is described in the section titled "Internal Control and Compliance Finding and Recommendation," that we consider to be a significant deficiency.

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 Treasury properly stated, in all material respects, the amounts recorded and reported in the Commonwealth's accounting and financial reporting system, Treasury's internal accounting and reporting systems, and supplemental information and attachments submitted to the Department of Accounts.

We noted a matter involving internal control and its operation and compliance with applicable laws, regulations, contracts, and grant agreements that requires management's attention and corrective action. This matter is described in the section titled "Internal Control and Compliance Finding and Recommendation."

Treasury has taken adequate corrective action with respect to the prior audit finding and recommendation identified as complete in the Findings Summary included in the Appendix.

Since the finding noted above has been identified as a significant deficiency, it 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 discussed this report with management at an exit conference held on February 4, 2025. Government Auditing Standards require the auditor to perform limited procedures on Treasury's response to the findings identified in our audit, which is included in the accompanying section titled "Agency Response". Treasury'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

EMS/clj

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	First Reported for Fiscal Year
Properly Perform and Document Retirement Benefits System Reconciliations	Complete	2022
Improve Vulnerability Management Process	Ongoing	2024

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

COMMONWEALTH of VIRGINIA
Department of the Treasury

DAVID L. RICHARDSON
TREASURER OF VIRGINIA

P.O. BOX 1879
RICHMOND, VIRGINIA 23218-1879
(804) 225-2142
FAX (804) 225-3187

February 6, 2025

Ms. Staci Henshaw
Auditor of Public Accounts
101 N. 14th Street, 8th Floor
Richmond, VA 23219

Dear Ms. Henshaw,

The Department of the Treasury (Treasury) welcomes the opportunity to respond to the recommendations in your Report on the Audit of the Department of the Treasury for the fiscal year ended June 30, 2024. Treasury appreciates the recognition of our progress in addressing previous concerns as noted in the report. Additionally, your comments and recommendations are appreciated and given the highest level of consideration by Treasury as we continually strive to improve our processes.

Comments to Management

Improve Vulnerability Management Process

Treasury will review its Threat Management Policy and align the vulnerability management process with the Security Standard. Treasury will work to mitigate the vulnerabilities and if Treasury is unable to mitigate the vulnerabilities an exception request will be submitted to VITA.

Sincerely,

David L. Richardson

David Richardson

cc: The Honorable Stephen E. Cummings, Secretary of Finance