



# DEPARTMENT OF THE TREASURY

## REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2025

Auditor of Public Accounts

Staci A. Henshaw, CPA

[www.apa.virginia.gov](http://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, 2025, 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; and
- one matter involving internal control and its operation requiring management's attention, that also represents an instance of noncompliance with applicable laws and regulations that is required to be reported under Government Auditing Standards; however, we do not consider the matter to be a material weakness.

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 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.

## - TABLE OF CONTENTS -

	<u>Pages</u>
AUDIT SUMMARY	
INTERNAL CONTROL AND COMPLIANCE FINDING AND RECOMMENDATION	1-2
RISK ALERT	3
INDEPENDENT AUDITOR'S REPORT	4-7
APPENDIX – FINDINGS SUMMARY	8
AGENCY RESPONSE	9

## INTERNAL CONTROL AND COMPLIANCE FINDING AND RECOMMENDATION

### **Improve Vulnerability Management Process**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**First Reported:** Fiscal Year 2024

The Department of Treasury (Treasury) continues not to 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 two vulnerabilities it detected in its vulnerability scans starting in August 2023. While Treasury submitted an exception request for the outstanding vulnerabilities affecting the web application since the prior year audit, the Commonwealth Security Risk Management (CSRM) division at the Virginia Information Technologies Agency (VITA) denied the exception request. Additionally, Treasury continues not to update its IS-07 Threat Management Policy to align with the current requirements of the Security Standard and Risk Management Standard, as it continues to reflect outdated requirements for installing security patches to mitigate vulnerabilities within 90 days.

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 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 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.

Software vulnerabilities are publicly known flaws that bad actors may exploit to circumvent organizational information security controls and 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, Treasury increases the risk of unauthorized access to sensitive and mission-critical systems.

Treasury created an internal Vulnerability Remediation Team in March 2025 that meets weekly to evaluate and remediate vulnerabilities based on vulnerability risk and severity as well as resource availability. While Treasury’s Vulnerability Remediation Team has made improvements in the agency’s

vulnerability management process, Treasury did not remediate the specific vulnerabilities affecting the web application because it prioritized mitigating vulnerabilities that it believed posed a greater risk to the agency's IT environment. Additionally, Treasury did not revise the Threat Management Policy's wording for the required timeframe to remediate vulnerabilities due to an oversight.

Treasury should review and revise its Threat Management Policy to ensure that its vulnerability management process aligns with the requirements outlined in the Security Standard and Risk Management Standard. Treasury should then implement its process to mitigate legitimate vulnerabilities affecting its IT environment within the timeframe required by its Threat Management Policy, the Security Standard, and Risk Management Standard. Timely remediation of significant vulnerabilities will help protect the confidentiality, integrity, and availability of Treasury's sensitive and mission-critical information.

## RISK ALERT

During the course of our audit, we encountered issues that are beyond the corrective action of Treasury's management alone and require the action and cooperation of management and VITA. The following issue represents such a risk to Treasury and the Commonwealth during fiscal year 2025.

### **Access to Centralized Audit Log Information**

**First Reported:** Fiscal Year 2024

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 the ITISP contract administrator, VITA is responsible for providing agencies with access to its security information and event management (SIEM) tool that stores information about historical security events throughout these components that may affect the Treasury's IT environment.

VITA and the ITISP contractors implemented the current SIEM tool in October 2023 after several unsuccessful iterations since 2018. While the current SIEM tool is storing audit logs for the ITISP infrastructure components, the SIEM tool does not present the information in a usable format that will allow agencies to adequately monitor their IT environments. Additionally, VITA does not configure the SIEM tool to give alerts about specific events captured in the audit logs. These alerts are necessary to provide Treasury with timely notification of potentially anomalous or malicious activity.

The Security Standard requires agencies to review and analyze audit records at least every 30 days for indications of inappropriate or unusual activity and assess any potential impact of the inappropriate or unusual activity. Using a SIEM tool without all necessary audit log information displayed to agencies reduces organizational security posture by not being able to react to and investigate suspicious system activity in a timely manner.

Treasury should continue to work with VITA to create relevant and usable information on the SIEM tool, including setting the appropriate alerts, 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 15, 2025

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, 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 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, 2025. 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 the audit finding from the prior report.

## **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.

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

\*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 not taken adequate corrective action with respect to the prior reported finding identified as ongoing 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, 2025. The Single Audit report will be available at [www.apa.virginia.gov](http://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 9, 2026. [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

ZLB/vks

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	Fiscal Year First Reported
Improve Vulnerability Management Process	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  
*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 10, 2026

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 recommendation in your Report on the Audit of the Department of the Treasury for the fiscal year ended June 30, 2025. 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 and revise its Threat Management Policy and align the vulnerability management process with the Security Standard. Treasury will mitigate the vulnerabilities or if Treasury is unable to mitigate the vulnerabilities an exception request will be submitted to VITA.

Sincerely,

A handwritten signature in black ink that reads "David L. Richardson".

David Richardson

cc: The Honorable Mark D. Sickles, Secretary of Finance