



# AGENCIES OF THE SECRETARY OF FINANCE

## 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

This report summarizes our fiscal year 2023 audit results for the following four agencies under the Secretary of Finance (Secretary):

- *Department of Accounts*
- *Department of Planning and Budget*
- *Department of Taxation*
- *Department of the Treasury and the Treasury Board*

Our audits of these agencies for the year ended June 30, 2023, found:

- proper recording and reporting of transactions, in all material respects, in the Commonwealth's accounting and financial reporting system, each agency's financial systems, and in supplemental information and attachments submitted to the Department of Accounts;
- ten findings involving internal control and its operations discussed in the Internal Control and Compliance Findings and Recommendations section, necessary to bring to management's attention;
- nine of the ten findings are considered to be instances of non-compliance with applicable laws and regulations that are required to be reported; and
- adequate corrective action with respect to prior audit findings 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 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.

This report also includes information on significant initiatives for the Secretary and Department of Accounts, including the status of the Commonwealth's Human Capital Management System development project and financial reporting changes for subscription-based information technology arrangements. In addition, it includes Risk Alerts, which are applicable to the Department of Accounts, Department of Planning and Budget, and Department of Taxation.

## – TABLE OF CONTENTS –

	<u>Pages</u>
AUDIT SUMMARY	
SIGNIFICANT INITIATIVES	1-2
Status of System Development Project	1
New Accounting Standard for Subscription-Based Information Technology Arrangements	2
INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS	3-10
Department of Accounts	3-6
Department of Planning and Budget	6-8
Department of Taxation	8-10
Department of the Treasury	10
RISK ALERTS	11-14
RETAIL SALES AND USE TAX COLLECTION AND DISTRIBUTION	15
INDEPENDENT AUDITOR’S REPORT	16-20
APPENDIX – FINDINGS SUMMARY	21
AGENCY RESPONSES	22-27
Department of Accounts	22-23
Department of Planning and Budget	24-25
Department of Taxation	26
Department of the Treasury	27

## SIGNIFICANT INITIATIVES

The following section provides an update on two major Commonwealth initiatives affecting Secretary of Finance agencies.

### Status of System Development Project

**Applicable to:** *Secretary of Finance and Department of Accounts*

#### *Commonwealth's Human Capital Management System Project*

In August 2016, Department of Accounts (Accounts) launched a payroll project to replace the Commonwealth's existing payroll system that has been in place since 1986. Accounts expanded this project in May 2018 to also replace the Commonwealth's human resources; time, attendance, and leave; and benefits administration systems for an all-encompassing Human Capital Management (Cardinal HCM) project. Accounts implemented the final release of the Cardinal HCM project in October 2022. Cardinal HCM currently serves over 231,000 users and 233 agencies.

Accounts estimated a total cost of \$135.8 million for the Cardinal HCM project. As of fiscal year 2023, Accounts spent approximately \$133.3 million to complete the project. The Governor authorized a working capital advance for the total estimated cost of the project. Accounts has drawn approximately \$145.9 million of the working capital advance to plan, develop, configure, and roll-out new software as of June 30, 2023. Due to the extended implementation period, the working capital advance included \$12.6 million for post-production support costs, which includes the cost of operating the system until fully implemented and agency billings could begin.

---

*Accounts implemented the final release of the Human Capital Management project in October 2022. Accounts has spent approximately \$133.3 million dollars on the project.*

---

The Cardinal HCM project integrated the Commonwealth's accounting and financial reporting system with the human resource, leave, and benefits functions. This integration reduced risks by replacing several aging statewide systems, improved performance with all Commonwealth system applications using cloud infrastructure, and fulfilled the majority of the Commonwealth's payroll and human resource requirements. Further, with the integration of the accounting and financial reporting system with the human resource, leave, and benefits functions, the Commonwealth has a variety of new reporting capabilities and more streamlined processes.

## New Accounting Standard for Subscription-Based Information Technology Arrangements

**Applicable to:** Department of Accounts

### *Governmental Accounting Standards Board Statement No. 96 SBITAs*

The Commonwealth implemented Governmental Accounting Standards Board (GASB) Statement No. 96, Subscription-Based Information Technology Arrangements (SBITAs) for fiscal year 2023. The statement provides guidance on the accounting and financial reporting for SBITAs, which is a contract that conveys control of the right to use another party's information technology software, alone or in combination with tangible capital assets. SBITAs include cloud computing arrangements such as software, platform, or infrastructure as a service. The statement requires governments to recognize a subscription liability for the amount owed on these contracts offset by a capitalized right-to-use asset. In the past, these arrangements were all expensed as paid. The statement does not apply to short-term agreements, less than 12 months, or perpetual agreements, which the government essentially owns. The accounting under this standard mirrors that in GASB Statement No. 87 for leases. SBITAs are essentially software leases. For fiscal year 2023, the Commonwealth's primary government reported \$145.1 million in long-term SBITA liabilities, with \$62.5 million due within one year, and \$197.9 million in right-to-use SBITA assets net of accumulated amortization in the Commonwealth's Annual Comprehensive Financial Report (ACFR). With the Commonwealth's initiative to eventually migrate all technology to cloud-based solutions, the SBITA assets and liabilities are expected to increase over the next several years.

---

*GASB Statement No. 96, SBITAs, is effective for fiscal year 2023. The Commonwealth's primary government reported \$145.1 million in long-term SBITA liabilities, with \$62.5 million due within one year, and \$197.9 million in right-to-use SBITA assets net of accumulated amortization.*

---

Being the largest user and contractor for information technology and services, we audited the Virginia Information Technologies Agency's implementation of GASB Statement No. 96 related to the Commonwealth's Information Technology Infrastructure Services Program and found material issues. The finding is included in our report entitled "Virginia Information Technologies Agency for the year ended June 30, 2023."

## INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

This section is organized by agency, and each finding reported includes information on the type of finding and the severity classification for the finding. The severity classifications are discussed in more detail in the section titled “Independent Auditor’s Report.”

### Department of Accounts

#### *Improve IT Risk Management and Contingency Planning Program*

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

Accounts does not conduct some aspects of its information technology (IT) risk management documentation in accordance with the Commonwealth’s Information Security Standard, SEC 501 (Security Standard). During fiscal year 2023, Accounts began addressing weaknesses in its IT risk management documentation by conducting an annual test of its Continuity Plan. However, Accounts did not conduct an annual review for 26 of its 27 systems’ System Security Plans (SSP) and does not include certain elements of information in all 27 SSPs. The information missing includes the system’s authorization boundary, information about the operational environment and relations with or connections to other systems, backup schedules, and the system’s security requirements.

The Security Standard requires Accounts to develop a security plan for the information system that includes these elements of information. Additionally, the Security Standard requires Accounts to review and update the SSPs on an annual basis or more frequently if necessary to address changes to the IT system and environment (*Security Standard, Section PL-2 System Security Plan*). Without annually reviewing, updating, and encompassing all the required elements in the system’s SSP, Accounts increases the risk that it will not effectively identify all potential risks and implement security controls needed to protect its sensitive system environment. Accounts did not review and update the SSPs in the last year to include the specific elements due to resource constraints and prioritizing other tasks.

Accounts should dedicate the necessary resources to conduct an annual review of its SSPs and include the specific elements of information that the Security Standard requires. This will help Accounts to identify potential risks and the need for security controls to protect the confidentiality, integrity, and availability of Accounts’ sensitive and mission-critical data.

#### *Improve Monroe IT Change and Configuration Management Process*

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

Accounts does not enforce its Monroe IT change and configuration management policy to conduct an explicit evaluation and approval of change requests from a security perspective, commonly referred to as a security impact analysis, for changes to some of its systems and applications. Accounts has two change management processes for its IT environment, the Paragon Change Process that applies

explicitly to the Commonwealth's enterprise resource planning system and the Monroe Change Process that applies to all other agency systems and applications.

Accounts' Configuration Management Policy, which is based on the Security Standard, requires the Information Security Officer (ISO) to analyze changes to the information system to determine the potential security impact prior to change implementation. The Configuration Management Policy also requires the ISO to approve configuration-controlled changes to the system with explicit consideration for security impact analyses (*Configuration Management Policy, Sections: B. Configuration Change Control, C. Security Impact Analysis; Security Standard, Sections: CM-3 Configuration Change Control and CM-4 Security Impact Analysis*). Without conducting and documenting a security impact analysis for each requested change, when applicable, Accounts may not detect and prevent changes that could compromise the security of the IT environment.

Accounts does not conduct a security impact analysis for applicable requests because it instead relies on its implementation of general IT security controls within its IT environment. Another contributing factor is that Accounts does not have an option, as part of its Monroe Change Process that applies to all other agency systems and applications, for the ISO to conduct and document a security impact analysis for applicable requested changes with subsequent approval or disapproval based on the analysis.

Accounts' ISO should conduct and document its analysis of security impacts for each change request prior to approval and implementation to the production IT environment. To assist with this requirement, Accounts should revise its Monroe Change Process that applies to all other agency systems and applications to include the ISO's documented analysis of potential security impacts and approval for each requested change. This will help to ensure the confidentiality, integrity, and availability of sensitive and mission essential data.

#### *Conduct Timely IT Security Audits*

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**First Issued:** 2022

Accounts continues to not perform IT security audits over its sensitive IT systems once every three years in accordance with the Commonwealth's IT Security Audit Standard, SEC 502 (Security Audit Standard). Since the 2022 fiscal year audit, Accounts retired two of the three sensitive systems previously noted as out of compliance. However, as of November 2023, Accounts has not had an IT security audit conducted over the third system, the Commonwealth's enterprise resource planning system, which has not had a comprehensive IT security audit conducted since July 2017.

The Security Audit Standard requires IT systems that contain sensitive data or reside in a system with a sensitivity of high for confidentiality, integrity, or availability be assessed at least once every three years (*Security Audit Standard, Sections: 1.4 Scope and Frequency of IT Security Audits and 2.1 Planning for IT Security Audits*). By not having IT security audits performed over sensitive systems once every three years, Accounts increases the risk for vulnerabilities in the configuration settings and deficient

management processes to go undetected and not effectively remediated. This reduces Accounts' security posture and increases the risk that malicious actors will exploit those vulnerabilities to gain unauthorized access to sensitive data.

Accounts did not include the Commonwealth's enterprise resource planning system in the audit scope for the Virginia Information Technologies Agency (VITA) Auditing Service's 2022 audit because of the agency's efforts to release the human resource and payroll management module. Additionally, Accounts originally planned to have an audit conducted over the Commonwealth's enterprise resource planning system in July 2023, but due to other technical projects affecting the Commonwealth's enterprise resource planning system, Accounts delayed the audit. As of November 2023, Accounts is finalizing a Statement of Work with an external contractor to conduct an IT security audit over the Commonwealth's enterprise resource planning system beginning in January 2024.

Accounts should continue its plans to have the external contractor conduct an IT security audit over the Commonwealth's enterprise resource planning system. Additionally, Accounts should work with VITA's Auditing Service to schedule and ensure performance of future security audits once every three years in accordance with the Security Audit Standard. This will help protect the confidentiality, integrity, and availability of Accounts' sensitive and mission critical data.

#### *Improve Database Security*

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

Accounts does not secure the database that supports the Commonwealth's enterprise resource planning system in accordance with its internal policies, the Commonwealth's Hosted Environment Information Security Standard, SEC 525 (Hosted Environment Security Standard), and industry best practices, such as the Center for Internet Security Benchmarks (CIS Benchmarks). We communicated two 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 it containing descriptions of security mechanisms.

The Hosted Environment Security Standard requires Accounts to implement certain security controls to safeguard systems that contain or process sensitive data. By not meeting the minimum requirements in the Hosted Environment Security Standard, Accounts cannot ensure the confidentiality, integrity, and availability within its system.

Accounts did not ensure the database's configuration and internal policies aligned with the Hosted Environment Security Standard and CIS Benchmarks due to dedicating its resources to perform a technical upgrade. Additionally, Accounts delayed revising its policies, procedures, and baseline configurations to align with the new Commonwealth security standard that will take effect in March 2024 and replace the Hosted Environment Security Standard.

Accounts should establish a process to file exceptions and obtain approval from the Commonwealth's Chief Information Security Officer when necessary. Accounts should also review and



update its internal policies and database configuration to ensure it aligns with the requirements of the Hosted Environment Security Standard and recommended settings in the CIS Benchmark or document the approved business justification for any deviations. This will protect the confidentiality, integrity, and availability of Accounts' sensitive and mission critical data.

## Department of Planning and Budget

### *Improve IT Risk Management and Contingency Planning Documentation*

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

The Department of Planning and Budget (Planning and Budget) developed a Continuity of Operations Plan (COOP) and Business Impact Analysis (BIA) that document recovery time objectives (RTO) and recovery point objectives (RPO) for its mission essential and primary business functions. However, Planning and Budget has established RTOs and RPOs that its contractual agreements with VITA do not support. VITA offers four separate tiers of disaster recovery services for executive branch agencies:

- Tier 1 – RTO less than or equal to four hours
- Tier 2 – RTO of five to 24 hours
- Tier 3 – RTO of 25 to 48 hours
- Tier 4 – RTO of 49 to 72 hours

If an agency does not subscribe to VITA's disaster recovery services, it is reliant on VITA's "best effort" to recover its servers, which occurs after VITA recovers the subscription tiers and is based on available daily backup data. The Security Standard requires Planning and Budget to provide the capability to restore information system components within the organization-defined restoration time-periods (*Security Standard, Section CP-10 Information System Recovery and Reconstitution CE (4)*).

Planning and Budget does not believe that VITA offered disaster recovery services meet their current needs, and as a result, has not contracted with VITA for any disaster recovery services. Without procuring the necessary services to meet the expected RTOs and RPOs for mission essential and primary business functions, Planning and Budget cannot guarantee the timely availability of its sensitive systems, potentially impacting critical services to citizens of the Commonwealth.

Planning and Budget should ensure its contractual agreements support the organization's RTO and RPO needs. If these contractual agreements cannot, it should revise its BIA and COOP to reflect the RTOs and RPOs that it can achieve and document its acceptance of risks for not meeting its original RTOs and RPOs.

## *Continue to Improve IT Change and Configuration Management Policy and Process*

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**First Issued:** 2021

Planning and Budget does not consistently implement its IT change and configuration management process as required by its Change Management Policy and the Security Standard. Since the prior year audit, Planning and Budget amended its Change Management Policy to align with the requirements of the Security Standard and resolve one of the two prior year weaknesses. Additionally, Planning and Budget is working with VITA to remediate the second prior year weakness, but due to delays by VITA's supplier, Planning and Budget does not have access to the centralized monitoring tool, which we communicated in a separate Risk Alert.

However, after conducting a sample of 40 changes that occurred within Planning and Budget's IT environment during the fiscal year, we found the following weaknesses:

- Planning and Budget did not document the Change Advisory Board's approval for all 40 sample changes. Planning and Budget's Change Management Policy requires the Change Advisory Board to meet regularly to review, assess, and authorize changes to be implemented into production (*Change Management Policy, "Charter and Planned Changes", Pg. 2; Security Standard, Section CM-3 Configuration Change Control*). While Planning and Budget maintains meeting minutes, it does not archive or attach the minutes to the changes discussed to verify approvals. Without documenting the proper approvals according to the Change Management Policy, Planning and Budget risks implementing unauthorized changes that could affect the availability or integrity of sensitive systems, compromising sensitive and financial data.
- Planning and Budget did not document its security impact analysis for 12 out of 40 (30 %) changes. Planning and Budget's Change Management Policy requires the developer to indicate the results of the risk analysis in the "Impact" tab of the change tracker. If the change has no impact, the developer should toggle "No" to indicate this in the "Impact" tab (*Change Management Policy, "Impact Tab" Pg. 16; Security Standard, Section CM-4 Security Impact Analysis*). Without indicating the impact of a change according to the Change Management Policy, Planning and Budget cannot ensure that it performs a risk analysis for each change. Additionally, without performing a security impact analysis, Planning and Budget may not detect and prevent the implementation of changes that compromise the security of its IT environment.
- Planning and Budget did not document test plans for 12 out of 40 (30 %) changes. Planning and Budget's Change Management Policy requires the testers or developers to document the date of the test, the individual performing the test, the test's description, and results (*Change Management Policy, "Impact Tab" Pg. 18; Security Standard, Section CM-4 Security Impact Analysis*). Without conducting and

documenting pre-implementation testing, Planning and Budget cannot validate the change will not cause disruption to its production environment when deployed.

While Planning and Budget made significant progress remediating the prior year weaknesses, developer oversight and Planning and Budget's lack of enforcing the formal process caused the weaknesses to exist. Planning and Budget should enforce its Change Management Policy to ensure its staff consistently document and implement changes to its IT environment to address the weaknesses listed above. This will help protect the confidentiality, integrity, and availability of Planning and Budget's sensitive and mission critical data.

#### *Allocate Resources to Enforce Separation of Duties*

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

Planning and Budget does not allocate the necessary resources to ensure separation of duties for key roles within its IT environment. Specifically, Planning and Budget designates the same employee to serve as the agency's ISO, the Chief Information Officer (CIO), and a developer.

The Security Standard requires that the ISO must not simultaneously serve the function of a CIO (*Security Standard, Section 2.4.1 Agency Head*). Having the ISO also serve as the CIO may limit effective assessment and necessary recommendations of security controls and assignment of security control responsibilities across the IT environment due to competing priorities that sometimes face the CIO. Planning and Budget's limited staffing caused the agency to designate the same employee in multiple roles.

Planning and Budget should allocate the necessary resources to dedicate separate individuals to the ISO and CIO roles and enforce separation of duties. This will help Planning and Budget to implement and maintain its information security program and controls as required by the Security Standard.

#### Department of Taxation

##### *Develop and Implement a Third-Party Service Provider Oversight Process*

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

The Department of Taxation (Taxation) does not have an effective, consistent, and documented process to identify, procure, maintain, and monitor external service providers (providers) that store, transfer, and process Taxation's mission critical and confidential data. As a result, Taxation does not have an accurate and complete listing of providers that Taxation managed alone and that VITA's Enterprise Cloud Oversight Service (ECOS) did not manage and monitor.

The Commonwealth's Hosted Environment Security Standard requires that agency management hold providers accountable for compliance with the Commonwealth's security standards through

documented agreements and oversight activities. Specifically, the Hosted Environment Security Standard requires Taxation to:

“... develop, document, and disseminate a system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.”

The Hosted Environment Security Standard also requires Taxation to have documented procedures and processes that facilitate the implementation of policies and associated controls. Lastly, the Hosted Environment Security Standard requires annual monitoring of the providers’ controls to ensure continued compliance with the Hosted Environment Security Standard and agency expectations (*Hosted Environment Security Standard, Sections 1.1. Intent, SA-1 System and Services Acquisition Policy and Procedures, SA-9 External Information System Services.*).

While Taxation’s Internal Audit Department reviews assurance reports from some providers every three years, the lack of an agency-wide list that is accurate and complete results in Taxation not reviewing some providers at all. Additionally, only reviewing the assurance reports every three years does not meet the Hosted Environment Security Standard requirement of performing annual reviews. Subsequently, providers’ internal control deficiencies may go undetected to Taxation for up to three years. The lack of documented policies and procedures that specifically address the contractual requirements that Taxation should consider before procuring providers’ services may result in Taxation not being able to hold providers accountable to the Hosted Environment Security Standard.

Taxation is aware of the weaknesses due to a previously issued Internal Audit finding and planned to have formal policies and procedures established by September 2023. However, Taxation delayed corrective actions due to limited resources and other higher-priority tasks. Additionally, the lack of a formal process led to Taxation not being able to confirm a complete list of its providers.

Taxation should develop and document policies and procedures that align with the requirements in the Hosted Environment Security Standard for procuring and monitoring providers. Taxation should then implement its formal process to consistently validate the effectiveness of providers’ security controls on an ongoing basis. Additionally, Taxation should identify and document in an agency-wide list its systems and services associated with providers, which will assist with monitoring providers. Effective provider oversight will help maintain the confidentiality, integrity, and availability of sensitive and mission critical data.

#### *Revoke Systems Access for Separated Employees in a Timely Manner*

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

Taxation did not timely revoke systems access for separated employees. Of the 128 terminated employees tested, Taxation did not timely remove access for 19 (14.8 %) separated employees due to delayed separation requests. Testing revealed that managers submitted separation requests between 2 and 142 days late. The delays in request submission were due to the managers being unaware of their

responsibilities and, in some instances, overlooking the need to submit a separation request. The Security Standard requires agencies to disable information systems access within 24 hours of termination (*Security Standard, Section PS-4 Personnel Termination*). Additionally, Taxation's internal policy requires access be removed no later than the employee's last workday.

Untimely removal of user access can compromise the integrity of Taxation's internal systems and increase the risk of unauthorized transactions. Taxation should timely revoke systems access for separated employees and should ensure that managers understand their responsibility for submitting separation requests timely.

## Department of the Treasury

### *Properly Perform and Document Retirement Benefits System Reconciliations*

**Type:** Internal Control

**Severity:** Deficiency

**First Issued:** Fiscal Year 2022

Since the prior audit, the Department of the Treasury (Treasury) Human Resources Department (Human Resources) has improved its process for retaining documentation of its review and assessment of reconciling items in the Commonwealth's human resources system cancelled records report and Virginia Retirement System's (Retirement System) automated reconciliation report as part of its monthly reconciliation between the Commonwealth's retirement benefits system and human resources system. However, Human Resources is not documenting and retaining support for its monthly reconciliation of creditable compensation between the Commonwealth's retirement benefits system and human resources system.

Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic 50470 requires agencies to perform a monthly reconciliation of creditable compensation between the Commonwealth's human resources and retirement benefits systems to ensure correct compensation information for all employees in the retirement benefits system. Retirement benefit system information is critical to the services provided by the Retirement System, and insufficient reconciliation of creditable compensation could result in improper payment of employee contributions to the Retirement System or errors in members' retirement-related data.

Human Resources' misunderstanding of the CAPP Manual requirements resulted in insufficiently documenting its reconciliation of creditable compensation amounts between the Commonwealth's retirement benefits system and human resources system. Human Resources should ensure it performs all retirement reconciliation requirements as outlined in the CAPP Manual Topic 50470 and should adequately retain documentation supporting the reconciliation process.

## RISK ALERTS

During the course of our audit, we encountered issues that are beyond the corrective action of management at an individual agency and require the action and cooperation of management at Accounts, Planning and Budget, Taxation, VITA, and other Commonwealth agencies. The following issues represent such a risk to these agencies and the Commonwealth during fiscal year 2023.

### Financial Reporting

**Applicable to:** *Department of Accounts*

Accounts relies on other Commonwealth entities (entities) to provide timely and accurate information to support the ACFR. Accounts requires 154 Commonwealth agencies and 44 component units to submit generally accepted accounting principles (GAAP) basis financial information (financial information) by specific deadlines. This allows Accounts time to compile, review, and submit the ACFR to the Auditor of Public Accounts (APA) for audit prior to December 15<sup>th</sup>, the Comptroller’s deadline for providing audited financial statements. Over the past several fiscal years, entities have increasingly submitted inaccurate and late financial information to Accounts. In fiscal year 2023, of the nineteen agencies and three component units we audited in support of the ACFR, thirteen entities had audit adjustments totaling \$2.4 billion; while in fiscal year 2022, nine entities had audit adjustments totaling \$3.2 billion. Audit adjustments relating to the Accounts’ ACFR compilation process totaled \$469.5 million in 2023 and \$229.1 million in 2022. Audit adjustment totals are reported gross and do not represent the impact on net position. Additionally, we have issued 25 internal control findings related to financial reporting (findings) between fiscal year 2019 and 2023 for ACFR-support audits. See the table below for the total findings issued by fiscal year and severity:

**Total Findings by Fiscal Year for ACFR Audits**

Table 1

	2023	2022	2021	2020	2019
<b>Material Weakness</b>	5	5	1	3	3
<b>Significant Deficiency</b>	1	1	2	2	2

We have noted similar issues for audits of entities outside of the ACFR-support audits.

**Total Findings by Fiscal Year for Non-ACFR Audits**

Table 2

	2023	2022	2021	2020	2019
<b>Material Weakness</b>	*	3	1	-	1
<b>Significant Deficiency</b>	*	2	2	1	2

\*Fiscal Year 2023 non-ACFR audits have not been performed as of the ACFR Deadline (12/15/2023).

Entities that have received a financial reporting material weakness finding between fiscal year 2019 and 2023 are as follows:

- Department of General Services\*\*
- Department of Health\*\*
- Department of Human Resource Management\*\*
- Department of Medical Assistance Services
- Department of Transportation
- Longwood University
- Old Dominion University
- University of Mary Washington
- University of Virginia, including the Medical Center\*\*
- Virginia Information Technologies Agency\*\*

\*\*2023 material weakness

The Code of Virginia § 2.2-803 and § 2.2-813, requires entities to submit financial information for the following reasons:

- The financial information required is necessary for Accounts to prepare the ACFR. Accounts must provide the audited ACFR by December 15<sup>th</sup>.
- Bond rating agencies use the ACFR to determine Virginia’s bond rating. Maintaining an unmodified opinion on the ACFR is critical to Virginia retaining its AAA bond rating.
- Bond rating agencies require inclusion of parts of the ACFR in bond offering statements.

To facilitate the Commonwealth complying with these requirements, Accounts requires entities to complete and submit financial information after fiscal year end. Accounts provides entities with guidance and instructions on how to report the financial information. Accounts compiles the financial information along with the financial data from the Commonwealth’s accounting and financial reporting system to create the ACFR. To ensure the accuracy of this information, the Comptroller’s annual directive requires that entities ensure internal controls are in place to avoid material misstatements and/or misclassifications in the financial information entities submit to Accounts.

Entities providing inaccurate and untimely information to Accounts may cause the Commonwealth not to meet the ACFR deadline, which could jeopardize the Commonwealth’s bond rating. While the Commonwealth corrected the information before issuance, it required the use of additional resources to detect and correct errors by both APA and Accounts, which limited the amount of time available to Accounts to prepare and the APA to audit the ACFR before the issuance deadline. As entities’ inaccuracies and late submissions increase, the time for Accounts to prepare the ACFR and APA to audit it is continually compressed, and it is becoming increasingly difficult to meet the December 15<sup>th</sup> deadline.

Some entities submitted late and/or inaccurate information to Accounts because they experienced a significant amount of turnover in key finance positions. As the Commonwealth

experiences difficulty in recruiting and retaining highly qualified staff, this turnover has created a knowledge gap in key financial positions. Additionally in recent years, the GASB has issued increasingly complex accounting standards requiring a more technical knowledge base in these finance positions. Limited staffing has led to entities lacking resources, including training on new and upcoming GASB standards and best practices in financial reporting, to incorporate new standards in the financial information. Furthermore, limited staffing has led to a lack of proper review of financial information by a knowledgeable independent individual.

While Accounts agrees there is a risk, it believes that because of its current staffing levels, there are limited actions it can take to address this risk for the Commonwealth. Accounts provides on-line training annually and meets with agencies experiencing the most difficulty with ACFR submissions to identify and remediate underlying issues. Additionally, Accounts offers annual open sessions for agencies to request training or additional information. According to Accounts, it is committed to stressing to entities' fiscal officers the importance of timely and accurate reporting, including the potential adverse impacts to the Commonwealth. However, Accounts does not have the staff available to provide detailed statewide guidance and training to agency personnel regarding the application of GASB standards. To compensate for these deficiencies, some entities have hired consultants or outside accounting professionals to assist their staff. The Secretary of Finance should consider if this is the most efficient and effective solution or whether a more statewide approach to the issue would be beneficial.

### Unpatched Software

**Applicable to:** *Department of Taxation*

**First Issued:** 2015

VITA contracts with various providers to create the Commonwealth's Information Technology Infrastructure Services Program (ITISP) to provide agencies with installation, maintenance, operation, and support of IT infrastructure components, such as servers, routers, firewalls, and virtual private networks. Taxation continues to rely on contractors procured by VITA for the installation of security patches in systems that support Taxation's operations. Additionally, Taxation relies on VITA as the contract administrator to maintain oversight and enforce contract agreements with the ITISP contractors. As of August 2023, the ITISP contractors had not applied a significant number of security patches that are critical and highly important to Taxation's IT infrastructure components, all of which are past the 90-day update window allowed by the Security Standard.

The Security Standard requires the installation of security-relevant software updates within 90 days of release. The Security Standard does allow for varying time periods depending on factors such as the criticality of the update, but generally the ITISP uses a 90-day window from the date of release as its standard for determining timely implementation of security patches (*Security Standard, Section: SI-2 Flaw Remediation*). Missing system security updates increases the risk of successful cyberattack, exploit, and data breach by malicious parties.

While VITA is responsible for enforcing the service level agreement, it has not been able to compel the current ITISP contractors to install certain security patches to Taxation's IT infrastructure to remediate vulnerabilities in a timely manner or take actions to obtain these required services from



another source. Taxation is working with VITA and the ITISP contractors to ensure that the ITISP contractors install all critical and highly important security patches on all servers. Additionally, our separate audit of VITA’s contract management will also continue to report on this issue.

### Access to Audit Log Monitoring Tool

**Applicable to:** *Department of Accounts & Department of Planning and Budget*

**First Issued:** 2021 (Accounts) 2023 (Planning and Budget)

Accounts and Planning and Budget (the agencies) rely on the Commonwealth’s ITISP to install, maintain, operate, and support IT infrastructure components, such as servers, routers, firewalls, and virtual private networks. As part of these services, the agencies rely on contractors procured by VITA to provide the agencies access to a centralized monitoring tool, known as the Managed, Detection, Response (MDR) Dashboard, that collects audit log information about activities in the agencies’ IT environments so that the agencies can review logged activity. Additionally, the agencies rely 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 access to the monitoring tool and audit log information for the last four years. As of October 2023, the MDR Dashboard went live for agencies to request access to the tool. However, VITA and the ITISP contractor did not formally communicate to all agencies that it was available and how to request access to the tool. Also, while the MDR Dashboard is in production, it does not include all audit log information 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 (*Security Standard, Section AU-6 Audit Review, Analysis, and Reporting*). VITA not enforcing the deliverable requirements with the ITISP contractors increases the risk associated with the Commonwealth’s data confidentiality, integrity, and availability.

The agencies are working with VITA and the ITISP contractors to obtain access to the audit log information within the MDR Dashboard to ensure the agencies can review the activities occurring in its IT environment in accordance with the Security Standard. Additionally, our separate audit of VITA will also address this issue.

## RETAIL SALES AND USE TAX COLLECTION AND DISTRIBUTION

In accordance with § 30-133.2 of the Code of Virginia, we perform work related to retail sales and use tax distributions as part of our annual audit of Taxation. As a part of our initial review, we established a one percent benchmark that Taxation should use to measure the effectiveness of the local sales and use tax distribution process. If the error rates exceed one percent, Taxation should perform additional analysis to determine the causes of the errors and whether further actions are required. Our audit included inquiries about the distribution and error processes and reviewed the error rate to ensure Taxation distributed the local sales and use taxes within the established benchmark.

In fiscal year 2023, Taxation collected approximately \$9.3 billion in retail sales and use taxes, with \$1.8 billion of these revenues being distributed to localities as a one percent local option tax. Taxation collects the tax and determines the local portion, which is distributed to the locality where the sale or activity occurred.

The sales and use tax distribution process requires a joint effort between Taxation, localities, and businesses. There are controls and processes in place to help ensure that locality distributions are accurate and made to the correct locality. When Taxation or localities detect a distribution error, they work together to research the error and, if necessary, Taxation processes an adjustment to correct the error and transfer the funds to the correct locality. Table 3 shows the local distribution amount for retail sales and use tax, as well as the amount and rate of distribution errors identified and corrected by Taxation in each of the last three fiscal years.

**Error Rate for Local Sales Tax Distributions**

Table 3

	2021	2022	2023
Local distribution amount	\$1,477,201,024	\$1,662,896,995	\$1,770,841,651
Errors identified and corrected	3,758,397	6,873,994	2,646,637
Error rate	0.25%	0.41%	0.15%

Source: Taxation’s financial accounting and reporting system

As shown above, the error rate for fiscal year 2023 was 0.15 percent. This is within the one percent benchmark established, which indicates Taxation is properly distributing the local portion of the retail sales and use tax. We do not recommend any changes in the established benchmark or to Taxation’s procedures for ensuring localities receive the correct distribution based on locality sales.



Staci A. Henshaw, CPA  
Auditor of Public Accounts

# Commonwealth of Virginia

*Auditor of Public Accounts*

P.O. Box 1295  
Richmond, Virginia 23218

December 15, 2023

The Honorable Glenn Youngkin  
Governor of Virginia

Michael Maul  
Department of Planning and Budget

Joint Legislative Audit  
And Review Commission

Craig M. Burns  
Department of Taxation

Stephen E. Cummings  
Secretary of Finance

David L. Richardson  
Department of the Treasury

Sharon H. Lawrence  
Department of Accounts

We have audited the financial records, operations, and federal compliance of the **Agencies of the Secretary of Finance** for the year ended June 30, 2023. 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 and Single 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 primary audit objectives for the audits of the Departments of Accounts, Planning and Budget, Taxation, and the Treasury for the year ended June 30, 2023, include the following:

- to evaluate the accuracy of financial transactions related to tax collections, including accounts receivable, unearned revenues and taxes, accounts payable and other liabilities, tax abatements, and tax and interest revenue as reported in the Commonwealth's accounting and financial reporting system and Taxation's accounting and financial reporting system and in supplemental information prepared by Taxation;

- to evaluate the accuracy of financial transactions related to cash and cash equivalents, investments, debt, and unclaimed property activity, which is controlled by Treasury as reported in the Commonwealth’s accounting and financial reporting system, Treasury’s internal systems and accounting records, and in supplemental information prepared by Treasury (including the activity of the Treasury Board, the Local Government Investment Pool, the Virginia College Building Authority, the Virginia Public School Authority, and the Virginia Public Building Authority);
- to evaluate whether the budget approved by the General Assembly is appropriately recorded in the Commonwealth’s accounting and financial reporting system and controls in this system are adequate to ensure program expenses do not exceed appropriations;
- to determine whether management has established and maintained internal controls over the Commonwealth’s financial reporting and other central processes and the centralized services provided to agencies and institutions in support of the preparation of the financial statements as indicated in the Audit Scope and Methodology section of this report;
- to determine whether management has established and maintained adequate operating and application system controls over the Commonwealth’s accounting and financial reporting, payroll, human capital management, budget, capital asset, and lease accounting systems and other internal systems as referenced in the Audit Scope and Methodology section;
- to determine whether the agencies have complied with applicable laws, regulation, contracts, and grant agreements;
- to test federal compliance in support of the Commonwealth’s Single Audit; and
- to review corrective actions related to audit findings from the prior year report.

### Audit Scope and Methodology

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.

### *Department of Accounts*

- Financial reporting\*
- Commonwealth’s accounting and financial reporting system
- Commonwealth’s payroll system
- Commonwealth’s human capital management system
- Commonwealth’s capital asset system
- Commonwealth’s lease accounting system
- Administrative activities
- Information security and general system controls (including access controls)

\*Including preparation of the Annual Comprehensive Financial Report and Schedule of Expenditures of Federal Awards.

### *Department of Planning and Budget*

- Budget execution
- Commonwealth’s budgeting system
- Information security and general system controls (including access controls)

### *Department of Taxation*

- Financial reporting
- Tax return processing
- Tax revenue collections
- Taxation’s accounting and financial reporting system
- Information security and general system controls (including access controls)

### *Department of the Treasury (including the Treasury Board operations)*

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

\*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.

The Virginia Board of Accountancy falls under the control of the Secretary of Finance; however, it is not material to the Annual Comprehensive Financial Report for the Commonwealth of Virginia. As a result, this agency is not included in the scope of this audit.

We performed audit tests to determine whether the 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 agencies’ operations. We confirmed cash, investments, and loan balances with outside parties. We performed analytical procedures, including budgetary and trend analyses, and tested details of transactions to achieve our audit objectives.

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 and federal compliance (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 as 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 or noncompliance 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 or material noncompliance with a type of compliance requirement of a federal program 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. We have explicitly identified nine findings in the section titled “Internal Control and Compliance Findings and Recommendations,” as significant deficiencies for the Commonwealth.

In addition to the significant deficiencies, we detected a deficiency in internal control that is not significant to the Commonwealth’s Annual Comprehensive Financial Report and Single Audit but is of sufficient importance to warrant the attention of those charged with governance. We have explicitly identified one finding in the section titled “Internal Control and Compliance Findings and Recommendations” as a deficiency.

## Conclusions

We found that Taxation properly stated, in all material respects, financial records reviewed in support of the tax collections activity detailed in the audit objectives as reported in the Commonwealth’s accounting and financial reporting system, Taxation’s accounting and financial reporting system, and supplemental information.

We found that Treasury properly stated, in all material respects, the financial records reviewed in support of the cash and cash equivalents, investments, debt, and unclaimed property activity reported in the Commonwealth’s accounting and financial reporting system, Treasury’s internal systems and accounting records, and supplemental information.

We found that the budget approved by the General Assembly is appropriately recorded in the Commonwealth’s accounting and financial reporting system, and controls in this system were adequate to ensure program expenses did not exceed appropriations.

We noted certain matters at Accounts, Planning and Budget, Taxation, and Treasury involving internal control and its operation and compliance with applicable laws and regulations that require management’s attention and corrective action. These matters are described in the section titled “Internal Control and Compliance Findings and Recommendations.”

The agencies of the Secretary of Finance have taken adequate corrective action with respect to prior audit findings and recommendations identified as complete in the Findings Summary included in the Appendix.

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, 2023. The Single Audit Report will be available at [www.apa.virginia.gov](http://www.apa.virginia.gov) in February 2024.

### Exit Conference and Report Distribution

We discussed this report with management of the respective agencies of the Secretary of Finance. Government Auditing Standards require the auditor to perform limited procedures on the agencies’ responses to the findings identified in our audits, which are included in the accompanying section titled “Agency Response”. The agencies’ responses were not subjected to the other auditing procedures applied in the audits and, accordingly, we express no opinion on the response. Additionally, VITA was made aware of the risk alerts and will respond to the issues in their separately issued audit report anticipated to be released in February 2023.

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

DBC/clj

## FINDINGS SUMMARY

Finding	Agency	Status of Corrective Action	First Issued
Ensure Adequate Resources are Available to Maintain Compliance with the Security Standard	Accounts	Complete	2022
Identify and Implement Critical Controls for the Commonwealth's New Human Resource and Payroll Management System	Accounts	Complete	2022
Prioritize Updates to the CAPP Manual Payroll Topics	Accounts	Complete	2022
Conduct Timely IT Security Audits	Accounts	Ongoing	2022
Improve IT Risk Management and Contingency Planning Program	Accounts	Ongoing	2023
Improve Monroe IT Change and Configuration Management Process	Accounts	Ongoing	2023
Improve Database Security	Accounts	Ongoing	2023
Continue to Improve IT Change and Configuration Management Policy and Process	Planning and Budget	Ongoing	2021
Improve IT Risk Management and Contingency Planning Documentation	Planning and Budget	Ongoing	2023
Allocate Resources to Enforce Separation of Duties	Planning and Budget	Ongoing	2023
Develop and Implement a Third-Party Service Provider Oversight Process	Taxation	Ongoing	2023
Revoke Systems Access for Separated Employees in a Timely Manner	Taxation	Ongoing	2023
Continue to Improve IT Risk Management Documentation	Treasury	Complete	2021
Properly Perform and Document Retirement Benefits System Reconciliations	Treasury	Ongoing	2022





## COMMONWEALTH of VIRGINIA

SHARON H. LAWRENCE, CPA, CGMA  
ACTING COMPTROLLER

Office of the Comptroller

P. O. BOX 1971  
RICHMOND, VIRGINIA 23218-1971

February 6, 2024

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

Dear Ms. Henshaw:

The Department of Accounts (Accounts) appreciates the opportunity to respond to the *Internal Control and Compliance Findings and Recommendations* contained in your 2023 Secretary of Finance Audit Report. We give your comments the highest level of importance and consideration as we continue to review and improve our current practices.

### **Internal Control and Compliance Recommendations**

#### *Improve IT Risk Management and Contingency Planning Program*

Accounts acknowledges the importance of System Security Plans (SSPs). Accounts is actively working to update all SSPs to conform with the Commonwealth's recently issued Information Security Standard, SEC 530, and expects to complete the needed updates by June 2024. Priority will be given to maintain updated SSPs for all agency sensitive systems.

#### *Improve Monroe IT Change and Configuration Management Process*

Accounts acknowledges the importance of conducting a Security Impact Analysis. Effective January 2024, Accounts implemented a Security Impact Analysis into the Monroe Change Management Process. Accordingly, the Information Security Officer must now review and approve the Security Impact Analysis before the change can be promoted to the production environment.

#### *Conduct Timely IT Security Audits*

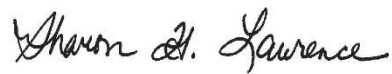
Accounts acknowledges the need for regular audits to ensure the integrity of sensitive information systems. Presently, Accounts has contracted with an approved vendor to perform an audit for the Commonwealth's enterprise resource planning system. The audit is underway with an expected March 2024 completion date. Accounts has confirmed with the Virginia Information Technologies Agency Auditing Service that the Commonwealth's enterprise resource planning system is included on the audit schedule for calendar year 2025.

Ms. Staci A Henshaw  
February 6, 2024  
Page 2

Improve Database Security

Accounts acknowledges the need to protect the confidentiality, integrity, and availability of sensitive and mission critical data. Presently, Accounts has a process in place to regularly file exceptions with the Commonwealth's Chief Information Security Officer for approval. Furthermore, Accounts is currently updating procedures to integrate the Center for Internet Security Benchmarks as appropriate.

Sincerely,



Sharon H. Lawrence

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



COMMONWEALTH of VIRGINIA  
*Department of Planning and Budget*

MICHAEL D. MAUL  
Director

1111 E. Broad  
Street Room 5040  
Richmond, VA 23219-1922

February 2, 2024

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

Dear Ms. Henshaw:

The Department of Planning and Budget (DPB) appreciates the opportunity to respond to the findings and recommendations contained in the 2023 Secretary of Finance Report. DPB has reviewed the findings and recommendations provided by the Auditor of Public Accounts (APA) as part of its audit of financial records and operations for the fiscal year that ended on June 30, 2023. I offer the following response to the internal control and compliance findings and recommendations for DPB.

**Internal Control and Compliance Findings and Recommendations**

**Improve IT Risk Management and Contingency Planning Documentation**

DPB acknowledges the importance of having a contingency planning process that is achievable and addresses the needs of each of its sensitive systems and the users of those systems. In response to this finding, DPB will continue to work with the Virginia Information Technologies Agency (VITA) to find solutions that address the APA finding and recommendation.

**Continue to Improve IT Change and Configuration Management Policy and Process**

DPB acknowledges that it needs to strengthen its internal controls to ensure that the agency complies with its change management policy and VITA standards. After this finding was first shared with DPB, the agency made internal policy and system changes to address this finding.

FAX (804) 225-3291

(804) 786-7455

TDD (804) 786-7578

Ms. Staci Henshaw  
February 2, 2024  
Page Two

*Allocate Resources to Enforce Separation of Duties*

DPB acknowledges the importance of separation of duties and the conflicts that exist in having the same employee act as both Information Security Officer (ISO) and Chief Information Officer (CIO). After this finding was first shared with DPB, the agency consulted with VITA, and we have since designated another agency employee as CIO.

DPB will use the findings and recommendations from the APA to continually improve its existing practices and policies. Thank you again for the opportunity to respond to your report.

Sincerely,

*Michael D. Maul*

Michael D. Maul  
Director

c: The Honorable Stephen E. Cummings  
Secretary of Finance



# COMMONWEALTH of VIRGINIA

## *Department of Taxation*

February 5, 2024

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

Dear Ms. Henshaw:

The Department of Taxation ("Virginia Tax") has reviewed the findings and recommendations provided by the Auditor of Public Accounts from your audit of the agency's financial records and operations for the year ended June 30, 2023. I appreciate the professionalism of your staff in the performance of the audit and the opportunity to provide the following response.

### **Risk Alert-Unpatched Software**

As your report documents, Virginia Information Technologies Agency (VITA) is responsible for ensuring this particular issue is addressed. However, Virginia Tax leadership formally communicates the status of this issue with VITA executive management each quarter. Virginia Tax will continue to assist VITA where possible regarding this issue.

### **Develop and Implement a Third Party Service Provider Oversight Process**

Virginia Tax will build out the supply chain risk management policy, standards, and related procedures to address the oversight of third-party service providers.

### **Revoke Systems Access For Separated Employees in a Timely Manner**

The Human Resources Director will remind supervisors of the importance of the timely revocation of systems access for separated employees. Additionally, the *Employee Separation Checklist* will be revised to instruct responsible supervisors to enter the revocation of systems access upon the notice of separation rather than the actual day of separation.

If you or your staff have any questions, please contact me at 804-786-3332.

Sincerely,

A handwritten signature in black ink, appearing to read "Craig M. Burns".

Craig M. Burns  
Tax Commissioner

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



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, 2024

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 Agencies of the Secretary of Finance for the fiscal year ended June 30, 2023. 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**

*Properly Perform and Document Retirement Benefits System Reconciliations*

Treasury has identified all the necessary pieces for the monthly reconciliation and developed a spreadsheet to assist in the reconciliations. Treasury will utilize the new spreadsheet and a checklist to ensure timely and documented completion of the monthly reconciliation.

Sincerely,

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

David Richardson

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