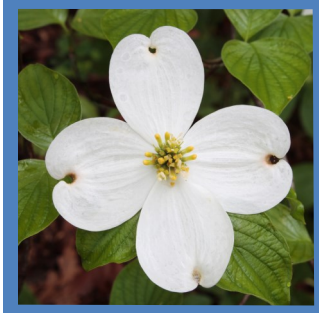



OFFICE OF THE ATTORNEY GENERAL AND DEPARTMENT OF LAW AND DIVISION OF DEBT COLLECTION

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2022

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

AUDIT SUMMARY

Our audit of the Office of the Attorney General and Department of Law (Office) and the Division of Debt Collection (Division) for the fiscal year ended June 30, 2022, included a review of internal controls over the following areas:

- Select human resource functions, including employment eligibility verification and executive leave management
- Operational expenses including payroll
- Division of Debt Collection
- Information system security

Relative to the areas tested, we found:

- proper recording and reporting of all transactions, in all material respects, in the Commonwealth's accounting and financial reporting system;
- matters involving internal control and its operation necessary to bring to management's attention; and
- instances of noncompliance with applicable laws and regulations or other matters that are required to be reported.

In the section titled "Audit Findings and Recommendations" we have included our assessment of the conditions and causes resulting in the internal control and compliance findings identified through our audit 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 developing and appropriately implementing adequate corrective actions to resolve the findings as required by the Department of Accounts in Section 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendations.

-TABLE OF CONTENTS-

AUDIT FINDINGS AND RECOMMENDATIONS

Improve Controls Over Payroll
Type: Internal Control
Repeat: No

We sampled various employees and payroll transactions to test the internal controls over payroll within the Office's Human Resources Department (Human Resources). Human Resources could not provide source documents to support various payroll transactions. In our review, we noted the following exceptions:

- For seven of seven salaried employees tested, Human Resources could not provide documentation supporting changes in gross pay.

- For one of two employees tested (50%), Human Resources could not provide complete documentation supporting the employee's overtime pay or evidence of approval.

- For 30 employees tested, the Office processed a total of 50 bonus payments. For 46 of the 50 bonus payments (92%), Human Resources could not provide documentation supporting the transactions.

- For five of five employees tested, Human Resources could not provide documentation supporting taxable income payments.

- For six of six employees tested, Human Resources could not provide documentation supporting Virginia Sickness and Disability Program payments.

- For 17 of 25 salaried employees tested (68%), Human Resources could not provide documentation supporting the employees' pay rates. Additionally, for 19 of the 25 employees (76%), Human Resources could not provide documentation supporting the employees' payroll coding.

- For eight of 20 separated employees tested (40%), supporting documentation for the termination and leave payout process was incomplete.

The Department of Human Resource Management Policy 6.10 – Personnel Records Management requires agencies to maintain complete and accurate records regarding each employee and position. Additionally, the Commonwealth Accounting Policy and Procedures (CAPP) Manual Topic 21005 – Records and Retention outlines the minimum record retention periods for audit support, including all records relating to payroll. The Department of Accounts and the Library of Virginia have established the minimum retention period for payroll files.

The failure to maintain proper documentation can result in unsupported changes in an employee's electronic file including pay rates, special payments, benefits, current position, and other sensitive information. This increases the risk of the Office processing inaccurate payments to employees.

Human Resources personnel were not consistently following the developed policies and procedures related to payroll documentation. Human Resources searched hardcopy personnel files and electronic records for requested documents. However, Human Resources did not properly retain the documents. A contributing factor to the lack of retention is that Human Resources experienced significant turnover during fiscal year 2022.

The Office should redesign policies and procedures to ensure staff properly file and consistently retain all payroll related documents supporting or approving employee overtime, special pays, leave payouts, and changes in pay rates. In addition, the Office should communicate the importance of document retention to staff and ensure the staff retain all payroll related documents in employees' payroll records in accordance with the CAPP Manual, Department of Human Resource Management, and Commonwealth retention policies.

Comply with Federal Regulations for Documentation of Employment Eligibility

Type: Internal Control and Compliance
Repeat: No

The Office's Human Resources Department did not properly complete Employment Eligibility Verification (I-9) forms in accordance with guidelines issued by the U.S. Citizenship and Immigration Services of the U.S. Department of Homeland Security. For one of 15 employees (7%), Human Resources was unable to provide I-9 documentation. Additionally, no record of the employee exists in E-Verify. Of the remaining 14 employees tested:

- Employee information in Section 1 did not match employee information in Section 2 of the I-9 form for three employees (21%).

- Human Resources did not complete the Preparer and/or Translator Certification Section for three employees (21%).

- Human Resources did not complete, and sign Section 2 of the I-9 form within three business days after the first day of employment for two employees (14%).

- The document(s) listed, which verifies the new employee's identity and employment eligibility, did not completely or accurately contain the required fields including the issuing authority, document number, and expiration date for three employees (21%).

- Human Resources did not create a case in E-Verify by the third business day after the employee started work for pay for three employees (21%).

- Human Resources did not create a case in the E-Verify system for one employee (7%).

Human Resources experienced significant staffing turnover during fiscal year 2022. The issues described above occurred under prior management and staff which left the Office between January 2022 and June 2022. While Human Resources refers to the U.S. Department of Homeland Security's Guidance for Completing Form I-9 Handbook for Employers, Human Resources did not have documented internal policies and procedures for completing I-9 forms. Additionally, Human Resources does not have a review process in place to ensure staff and newly hired employees complete I-9 forms accurately and timely.

The Immigration Reform and Control Act of 1986 requires that all employers complete an I-9 form to verify both identity and employment eligibility for all employees hired after November 6, 1986. Additionally, the U.S. Department of Homeland Security's Guidance for Completing Form I-9 Handbook for Employers prescribes federal requirements for completing I-9 forms. Lastly, Section 40.1-11.2 of the Code of Virginia requires all agencies of the Commonwealth to use the E-Verify program for each newly-hired employee who is to perform work within the Commonwealth. Not complying with federal requirements could result in civil and/or criminal penalties for both the employee and employer in addition to debarment from government contracts.

Human Resources should ensure all staff and newly hired employees complete I-9 forms in accordance with the U.S. Department of Homeland Security guidelines. Human Resources should develop, document, and implement policies and procedures for proper completion of I-9 forms. In addition, management should provide adequate training to personnel responsible for completing I-9 forms to ensure compliance with the applicable federal and state requirements.

Continue to Improve Firewall Management

Type: Internal Control and Compliance

Repeat: Partial (first issued in fiscal year 2016 with significant progress)

The Office does not properly secure the firewall that safeguards its internal network in accordance with the Commonwealth's Information Security Standard, SEC 501 (Security Standard). We communicated two control weaknesses to management in a separate document marked Freedom of Information Act (FOIA) Exempt under Section 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The Security Standard requires the documentation and implementation of certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of the Office's information systems and data.

The Office did not complete the documentation and implementation of certain security controls due to a lack of resources and clearly defined processes and procedures. The Office should develop a plan to implement the controls discussed in the communication marked FOIA Exempt in accordance with the Security Standard in a timely manner. Doing this will help to ensure the Office secures its network to protect its systems and data.

Continue to Improve Virtual Private Network Security Controls

Type: Internal Control and Compliance

Repeat: Partial (first issued in fiscal year 2019 with significant progress)

The Office has made significant progress since our previous review by updating its Information Security Program Policies (Security Policies) to align with the requirements of the Security Standard. However, three weaknesses continue to exist in the Office's Virtual Private Network (VPN). We identified and communicated the specific control weaknesses to management in a separate document marked FOIAE under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

The Office did not complete the necessary procedures to facilitate the implementation and management of its policies and controls due to limited staffing. The Office should dedicate the necessary resources to mitigate the specific risks communicated in the FOIAE document to improve the security posture of remote connections and to comply with the Security Policies and the Security Standard. The fiscal year 2023 audit will include an evaluation of the Office's completed corrective action and determine whether the Office satisfactorily resolved the weaknesses.

Independently Align the Information Security Officer

Type: Internal Control and Compliance

Repeat: No

The Office does not position the Information Security Officer (ISO) role in an organizationally independent unit from the Chief Information Officer (CIO). The Security Standard states that the ISO must be a Commonwealth of Virginia employee, the ISO shall report directly to the agency head, and the ISO must not simultaneously serve the function of CIO (*Security Standard Section: 2.4.1 Agency Head*). Having the ISO role report to the CIO may limit effective assessment and necessary recommendations of security controls and assignment of security control responsibilities across the information technology (IT) environment due to possible competing priorities that sometimes face the CIO.

Staffing issues resulted in the Office maintaining a single position that filled both the role of Director of IT/CIO and the role of ISO. In May 2023, the Office hired one of its contractors as a full-time Commonwealth of Virginia employee to fill the role of ISO/Project Manager. However, in the current reporting structure, the ISO/Project Manager reports to the Director of IT/CIO to facilitate his project management responsibilities.

The Office should evaluate the organizational placement of the ISO/Project Manager to eliminate any potential conflicts of interest in the implementation of its information security program and controls. While it may not be feasible to have the ISO/Project Manager report directly to the agency head, the Office should consider placing the ISO role in a different organizational unit reporting to another executive-level position. Doing this will provide the necessary segregation of duties to help ensure that the ISO effectively assesses and recommends security controls, in addition to assigning security control responsibilities.

Develop and Implement a Process to Maintain Oversight Over Service Providers

Type: Internal Control and Compliance

Repeat: No

The Office is not gaining assurance that all information technology service providers (IT providers) have effective operating controls to protect the Office's sensitive and confidential data either during initial service procurement or on an ongoing basis after initial service procurement. The Office's Security Policies and the Commonwealth's Hosted Environment Information Security Standard, SEC 525 (Hosted Environment Security Standard) require that the Office define, document, and implement requirements and processes to gain assurance over IT providers. IT providers are organizations that perform certain business tasks or functions on behalf of the Office. The Office has three IT providers that transmit, process, or store sensitive and mission-critical data. Specifically, our review identified the following issues:

- The Office does not maintain a complete, up-to-date list of IT providers that perform business tasks or functions on behalf of the Office. During our review, the Office provided a list of IT providers that included one provider; however, the Office later identified two additional service providers that process sensitive agency data. *(Hosted Environment Security Standard, Section CA-3-COV and sub-sections)*.

- The Office does not define and document agency and IT provider roles and responsibilities in its contracts with vendors as required by internal policy and the Hosted Environment Security Standard. (*Security Policies, Section SA-9 (b); Hosted Environment Security Standard, Section SA-9 (b))*

- The Office does not document enforceable agreements with each IT provider that requires submission of monthly service reports and annual independent audit assurance reports. *(Security Policies, Section SA-9(a); Hosted Environment Security Standard, Sections SA-4 and SA-9 (a))*

- The Office does not obtain and review monthly service reports from each IT provider. *(Hosted Environment Security Standard, Sections SA-9 and SA-9-COV-3 (1).)*

- The Office does not obtain and review annual independent audit assurance reports, such as System and Organization Controls reports, to determine deficiencies and the potential need to implement complementary or compensating controls. *(Hosted Environment Security Standard, Sections SA-9 and SA-9-COV-3 (1).)*

By not defining and employing a process to gain assurance over its IT providers' operating controls, the Office cannot validate that the providers have effective security controls to protect the Office's sensitive and confidential data, increasing the chance of a breach or possible data disclosure. Additionally, by not documenting an annual review of independent audit assurance and implementing possible compensating controls for each IT provider, the Office does not ensure an adequate level of security controls, thus putting its sensitive data at risk.

Prior to July 2023, the Office did not have a policy addressing IT provider oversight requirements. On July 1, 2023, the Office completed their Information Security Program Policies, which include System and Services Acquisition requirements. However, the Office has not completed procedures that document the process the Office must follow to implement the policy requirements and any associated controls. Therefore, the Office has not developed and implemented a process for gaining assurance over outsourced operations due to the absence of a documented procedure.

The Office should develop and document a procedure and process to maintain oversight over IT providers. The Office should communicate required security controls to its IT providers through documented agreements with the IT providers, as appropriate. The Office should then request and evaluate monthly service reports and annual independent audit assurance reports from each IT provider to ensure the IT provider has effective operating controls to protect the Office's sensitive and confidential data. During the evaluation, the Office should identify control deficiencies, develop mitigation plans, and escalate issues of non-compliance, as needed. Finally, the Office should document its evaluation of the monthly service reports and annual assurance reports from each IT provider. Gaining sufficient assurance over IT provider's security controls will help to ensure the confidentiality, integrity, and availability of sensitive data.

Improve Information Security Program and IT Governance

Type: Internal Control and Compliance

Repeat: Partial (first issued in 2021 with significant progress)

The Office made significant progress since our previous review by hiring an ISO, procuring external consulting services, and dedicating more resources to its information security program. However, as the Office continues to address past findings to mature its information security program and IT governance structure, several outstanding findings remain in addition to new findings we have identified, that need immediate attention to bring the Office's information security program in compliance with the Security Standard.

Specifically, as noted in the findings above, the Office continues to have internal control weaknesses related to information security procedures, network firewall configurations, and virtual private network configurations. In addition, this year's review found that the Office has internal control weaknesses related to service provider oversight and the ISO reporting structure. The Office resolved the following control weaknesses from our prior review that did not meet the requirements of the Security Standard:

- Information Security Policies
- Database System Configurations
- Logging and Monitoring Processes
- Change Control Process
- Access Approval and Authorization Processes

Agency heads are responsible for ensuring that their agency maintains, documents, and effectively communicates a sufficient information security program to protect the agency's IT systems (*Security Standard, Section 2.4.2*). Not having a mature governance structure to properly manage the agency's IT environment and information security program can result in a data breach or unauthorized access to confidential and mission critical data leading to data corruption, data loss, or system disruption if accessed by a malicious attacker, either internal or external.

Until recently, a lack of IT resources hindered the Office's ability to consistently and timely remediate internal control weaknesses from findings issued in our previous audits. Additionally, prior to July 2023, the Office did not have a policy detailing control requirements. Therefore, the Office has not yet implemented all the control requirements outlined in the Office's Security Policies.

The Office should continue to create and implement information security procedures to facilitate the requirements detailed in its Information Security Program Policies. The Office should also continuously evaluate its IT resource levels to ensure sufficient and appropriate resources are available to implement IT governance changes and correct the remaining control weaknesses. Implementing these recommendations will help ensure the confidentiality, integrity, and availability of the Office's mission-essential data.

AGENCY HIGHLIGHTS

The Attorney General is the chief executive officer of the Commonwealth of Virginia's Department of Law. The Office of the Attorney General and Department of Law (Office) acts as the Commonwealth's law firm. The Attorney General and his staff represent the Commonwealth's interests in all civil cases naming the Commonwealth, or any of its agencies or officials, as a party, and in criminal cases on appeal to the Court of Appeals of Virginia and the Supreme Court of Virginia. In cases involving federal law, the Attorney General represents the Commonwealth's interests in federal court. The Office also enforces consumer protection laws and investigates Medicaid fraud.

The Attorney General is also the legal advisor to the Governor and more than 200 state agencies, boards, commissions, and institutions. The Attorney General renders official opinions on the application of the law upon written request of the Governor, members of the General Assembly, members of the judiciary, state officials, or local constitutional officers. The Office handles criminal convictions on appeal and defends the state when prisoners sue concerning their incarceration. In addition, the Office defends legal challenges of the constitutionality of state laws. The Attorney General is responsible for providing all legal services for the Commonwealth and its agencies unless it is impracticable and uneconomical to do so. If the Commonwealth utilizes outside counsel, the Attorney General supervises the appointment and payment of private attorneys hired by other state agencies for various matters.

The Office's organizational structure is similar to a private law firm, with divisions devoted to legal specialties. In addition to the main office in Richmond, there are regional offices in Abingdon, Fairfax, Hampton Roads, and Roanoke. The Administration Division provides finance, human resources, information technology, and operations support to the legal divisions.

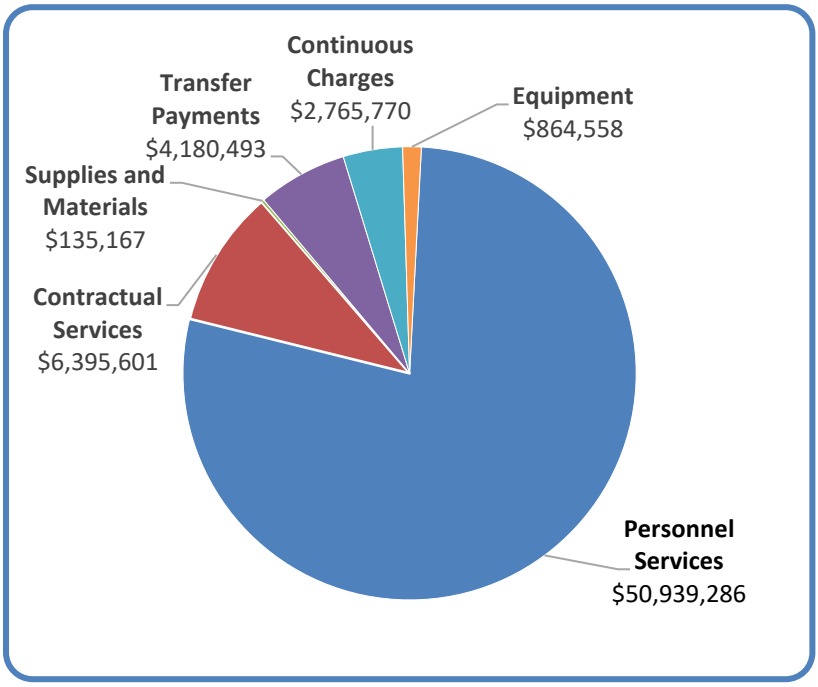
Expenses

Chart 1 on the following page provides a breakdown of total operational expenses by type for all funds for fiscal year 2022 for both the Office and the Division of Debt Collection (Division). Personnel services are the largest expense type and increased from $45.6 million in fiscal year 2021 to $50.9 million in fiscal year 2022. Therefore, we included internal controls over the payroll cycle as one of our audit objectives for fiscal year 2022. We also included procedures to ensure compliance with federal and state employment eligibility verification regulations and executive leave management.

The Office experienced significant turnover during fiscal year 2022. There were 123 new employees hired during fiscal year 2022 compared to 51 new employees in fiscal year 2021. The large number of new employees and separating employees resulted in an increased workload for the Human Resources Department, which experienced turnover in all five positions during the fiscal year.

Operational Expenses by Type for Fiscal Year 2022

Chart 1



Source: Commonwealth accounting and financial reporting system

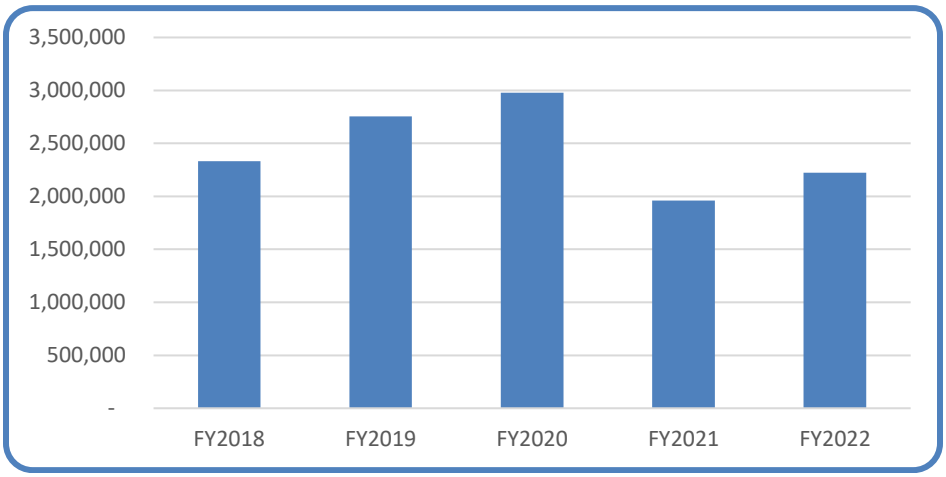
Division of Debt Collection

The Division is a separate agency within the Office. The Division collects delinquent accounts for state agencies and state-supported institutions of higher education and their hospitals. Upon receiving delinquent accounts from state agencies, the Division will take appropriate action, including litigation, to collect.

The Division retains up to 30 percent of any funds recovered on behalf of the Commonwealth, as well as any separate attorney's fees awarded to the Commonwealth. The Division uses these funds to pay operating costs. At the conclusion of each fiscal year, the Division retains up to $400,000 as operating capital and transfers any excess amounts to the General Fund of the Commonwealth.

Debt Collection Fees

Chart 2



Source: Commonwealth's accounting and financial reporting system

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

January 9, 2024

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

The Honorable Jason S. Miyares
Attorney General of Virginia

We have audited the financial records and operations of the **Office of the Attorney General and Department of Law and Division of Debt Collection** (Office) for the year ended June 30, 2022. We conducted this performance audit in accordance with generally accepted government auditing standards. 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 objectives were to evaluate the accuracy of recorded financial transactions in the Commonwealth's accounting and financial reporting system, review the adequacy of the Office's internal controls, test compliance with applicable laws, regulations, contracts, and grant agreements and review corrective actions of audit findings from prior year reports. See the Findings Summary included in the Appendix for a listing of prior year findings and the status of follow-up on management's corrective action.

Audit Scope and Methodology

The Office'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 significance and risk in determining the nature and extent of our audit procedures. Our review encompassed controls over the following significant cycles, classes of transactions, and account balances.

Employment eligibility verification
Executive leave management
Operational expenses including payroll
Division of Debt Collection
Information system security

We performed audit tests to determine whether the Office's controls were adequate, had been placed in operation, and were being followed. Our audit also included tests of compliance with provisions of applicable laws, regulations, contracts, and grant agreements. Our audit procedures included inquiries of appropriate personnel, inspection of documents, records, and contracts, and observation of the Office's operations. We performed analytical procedures, including trend analyses. We also tested details of transactions to achieve our 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.

Conclusions

We found that the Office properly stated, in all material respects, the amounts recorded and reported in the Commonwealth's accounting and financial reporting system. The financial information presented in this report came directly from the Commonwealth's accounting and financial reporting system.

We noted certain matters involving internal control and its operation and compliance with applicable laws, regulations, contracts, and grant agreements that require management's attention and corrective action. These matters are described in the section titled "Audit Findings and Recommendations."

The Office has not taken adequate corrective action with respect to audit findings noted as repeat in the Findings Summary included in the Appendix. The Office has taken adequate corrective action with respect to audit finding noted as resolved in the Findings Summary.

Exit Conference and Report Distribution

We discussed this report with management on January 25, 2024. Management's response to the findings identified in our audit is included in the section titled "Agency Response." We did not audit management's response and, accordingly, we express no opinion on it.

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

JMR/vks

FINDINGS SUMMARY

Finding Title	Status of Corrective Action	First Issued
Improve Database Security	Complete	2021
Improve Controls Over Payroll	Ongoing	2022
Comply with Federal Regulations for Documentation of Employment Eligibility	Ongoing	2022
Continue to Improve Firewall Management	Ongoing	2016
Continue to Improve Virtual Private Network Security Controls	Ongoing	2019
Independently Align the Information Security Officer	Ongoing	2022
Develop and Implement a Process to Maintain Oversight Over Service Providers	Ongoing	2022
Improve Information Security Program and IT Governance	Ongoing	2021

COMMONWEALTH of VIRGINIA

Office of the Attorney General

Jason S. Miyares
Attorney General

202 North Ninth Street
Richmond, Virginia 23219
804-786-2071
Fax 804-786-1991
Virginia Relay Services
800-828-1120
7-1-1

January 25, 2024

The Auditor of Public Accounts
P. O. Box 1295
Richmond, Virginia 23218

Dear Ms. Henshaw:

On behalf of the Attorney General Jason S. Miyares and the Office of the Attorney General I would like to thank you for providing us an opportunity to comment on the findings and recommendations in the Fiscal Year 2022 audit of the Office of the Attorney General.

I am very pleased that you and your team "found that Office properly stated, in all material respects, the amounts recorded and reported in the Commonwealth's accounting and financial reporting system."

Management recognizes the need to continue to strengthen our internal controls and compliance with all sections of SEC 501 and for the areas identified for Information Technology Section. We are actively working towards redressing the concerns noted in the prior audit report and this current audit report. Management also recognizes the need to strengthen internal controls and compliance in other areas of the Agency. We have worked to redress the areas of Human Resources and Payroll in this current audit report.

As always, management of this agency continues to recognize the need for compliance with applicable standard and requirements, and for adequate internal controls and polices to ensure security and compliance by our agency. We will work expeditiously to address the items you have noted.

Sincerely,

Chuck Slemp
Chief Deputy Attorney General

THE OFFICE OF THE ATTORNEY GENERAL
AND DEPARTMENT OF LAW AND DIVISION OF DEBT COLLECTION

As of June 30, 2022

Jason S. Miyares
Attorney General

Chuck Slemp
Chief Deputy Attorney General

Darrell H. Jordan, Jr.
Chief of Staff

Christie A. Wells
Chief Finance Officer