

Virginia Auditor of Public Accounts

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

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2025

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, 2025, consisted of a review of internal controls over the following areas: operational expenses, grant administration, legal services billings, legal settlements, the Division of Debt Collection, and information system security. We found:

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

In addition, we found adequate corrective action with respect to the prior audit finding identified as complete in the [Findings Summary](#) included in the Appendix. We did not include two prior findings in the scope of our audit as per inquiry with management, we determined that corrective action was ongoing as of June 30, 2025.

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 Topic 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

	<u>Pages</u>
AUDIT SUMMARY	
INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS	1-3
AGENCY HIGHLIGHTS	4-7
INDEPENDENT AUDITOR'S REPORT	8-10
APPENDIX – FINDINGS SUMMARY	11
AGENCY RESPONSE	12-15

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Threat Management and Incident Response Program

Type: Internal Control and Compliance

The Office of the Attorney General and Department of Law (Office) does not conduct certain elements of its threat management and incident response program in accordance with the Commonwealth's Information Security Standard, SEC530 (Security Standard), as well as the Office's Information Security Program Policies (Office Policy) and Information Security Program Official Procedures (Office Procedures). Specifically, the following weaknesses exist:

- The Office does not have an Incident Response Plan. Without a documented Incident Response Plan that includes all required elements, the Office may not consistently identify or respond to security incidents.
- The Office does not designate an Information Security Incident Response Team for responding to cyber-attacks. The Office uses various tools and services for threat detection and monitoring but has not established a formal incident response team. Without establishing an Information Security Incident Response Team, the Office may not detect, contain, and recover from cyber incidents quickly and effectively.
- During the fiscal year under review, the Office did not protect information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion. Not protecting information from intrusion monitoring tools increases the risk of attackers altering monitoring data to mask or hide malicious actions, as well as loss of forensic evidence and investigative capability. As of July 2026, the Office added a file integrity monitoring service to protect information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion.
- The Office does not consistently implement its documented process to track, prioritize, and categorize incidents in a service desk ticket. The Office's Information Technology (IT) Service Level Policy requires that the Office open a service desk ticket for service requests for all problems, including threats to data integrity or computer security. Ticketing systems provide structured workflows for prioritization, assignment, and resolution. Without consistently tracking information security incidents in its service desk ticketing system, the Office's response actions may be inconsistent, incomplete, or untracked, hindering rapid detection, analysis, and coordination across teams and increasing the time to resolve the incident.
- The Office does not review and update the Office Policy and Office Procedures on an annual basis. Specifically, the Office has not reviewed and updated the Office Policy and Office Procedures since July 2023. As a result, the Office bases its information security policies and procedures on the Information Security Standard, SEC501, which is no longer valid. The

Commonwealth's Information Security Standard, SEC530, superseded SEC501 as of March 2024. Without regularly reviewing and updating the Office Policies and Office Procedures, the Office may inconsistently design and implement the incident response program and increase the risk of mismanaging security incidents.

- The Office does not adequately document procedures that detail its threat detection practices, logging and monitoring processes, incident handling practices, and mitigation measures used. By not documenting these practices and processes, the Office increases the risk of not effectively detecting incidents and administrators not consistently monitoring and responding to potential security events.

The Office does not have a process to annually review and revise its Office Policy and Office Procedures, which led to outdated Office Policy and Office Procedures. In addition, the Office does not have an individual responsible for maintaining current information security policies and procedures. Further, turnover in the Information Security Officer (ISO) role contributed to the Office not conducting certain elements of its threat management and incident response program in accordance with the Security Standard, Office Policy, and Office Procedures.

The Office should develop and document an Incident Response Plan that provides a roadmap for implementing all of the required elements. The Office should designate an Information Security Incident Response Team for responding to cyber-attacks; consistently implement its documented process to track, prioritize, categorize, and respond to incidents; and document its threat detection practices, logging and monitoring processes, incident handling practices, and mitigation measures used. Finally, the Office should develop a process to annually review and update its Office Policy and Office Procedures, then review and update the Office Policy and Office Procedures to align with the requirements in the Security Standard. Improving the threat management and incident response program will help ensure the Office appropriately responds to malicious attempts to compromise confidentiality, integrity, and availability of sensitive information.

Continue to Improve Virtual Private Network Security Controls

Type: Internal Control and Compliance

First Reported: Fiscal Year 2019

The Office has made progress since the prior audit by resolving one of the two identified control weaknesses. However, the Office continues to not fully implement a required security control for its Virtual Private Network (VPN) in accordance with the Office Policy, as well as the Security Standard. We communicated one control weakness 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.

Not implementing all required security controls for the VPN increases the risk for a malicious user to exploit an existing vulnerability or weakness and cause a system compromise or unavailability. The

Office's previous employees did not appropriately implement the control. The Office has onboarded new employees and should implement the security control mentioned in the FOIAE communication to ensure the VPN aligns with its Office Policy as well as the Security Standard. Implementing this control will help maintain the confidentiality, availability, and integrity of the Office's sensitive and mission-critical data.

Improve Server Operating System Security

Type: Internal Control and Compliance

First Reported: Fiscal Year 2024

The Office made progress since the prior audit by resolving one of the five identified control weaknesses. However, the Office continues to not implement certain controls and processes on the operating system that supports a sensitive Office server to properly secure the server in accordance with the Office Policy, the Office Procedures, the Security Standard, the Commonwealth's IT Risk Management Standard, SEC520 (Risk Management Standard), and industry best practices, such as the Center for Internet Security's Benchmark (CIS Benchmark). We identified and communicated four weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

Lack of resources, personnel changes, and configuration errors by Office staff contributed to the issues. Without these controls, the Office may not effectively and consistently protect and mitigate risks to data.

The Office should ensure server operating system configurations, controls, and processes align with the requirements in the Office Policy, Office Procedures, the Security Standard, Risk Management Standard, and the CIS Benchmark. Implementing these controls will help maintain the confidentiality, integrity, and availability of the sensitive and mission-critical data stored or processed on the server.

AGENCY HIGHLIGHTS

The Attorney General is the chief executive officer of the Commonwealth of Virginia's Department of Law. The 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 Office receives and administers legal settlements that stipulate the terms by which the Commonwealth will receive funds in conjunction with the Code of Virginia.

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 uses outside counsel, the Attorney General supervises the appointment and payment of private attorneys hired by other state agencies for various matters.

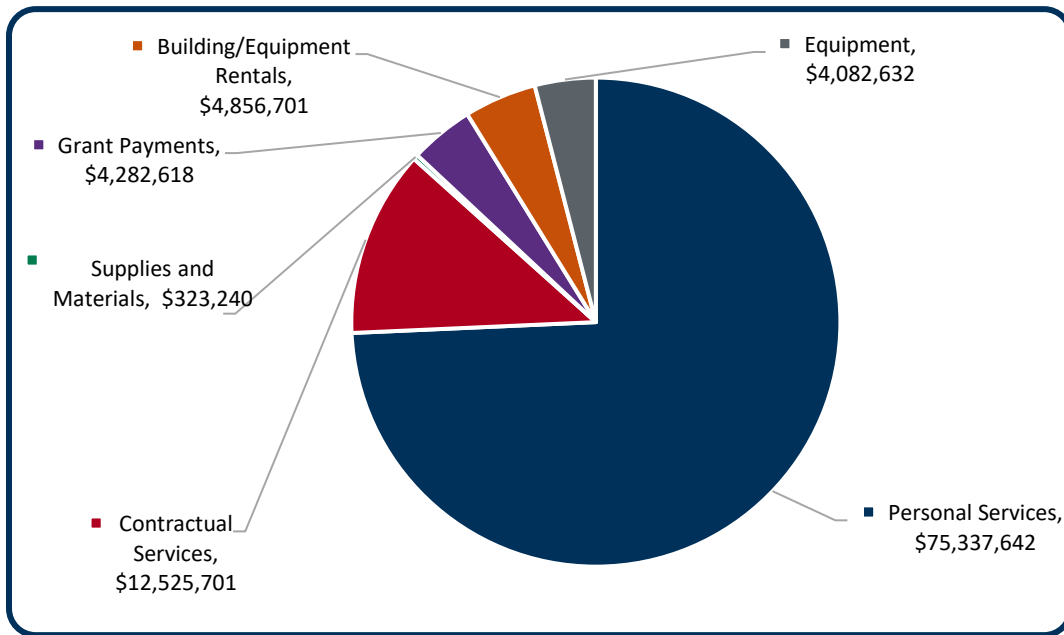
The Office's organizational structure is like a private law firm, with divisions devoted to legal specialties. In addition to the main office in Richmond, there are regional offices in Abingdon, Fairfax, Hampton Roads, and Roanoke. The Administration Division provides finance, human resources, information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

Expenses

Chart 1 provides a breakdown of total operational expenses by type for all funds for fiscal year 2025 for both the Office and the Division of Debt Collection (Division). Expenses increased from \$97.7 million in fiscal year 2024 to \$101.4 million in fiscal year 2025. This expense increase was primarily attributable to a \$4.1 million increase in personal services, which is the result of a statewide salary increase of three percent and an increase in the legal billing rate during the year for outside counsel's services.

Operational Expenses by Type for Fiscal Year 2025

Chart 1



Source: Commonwealth accounting and financial reporting system

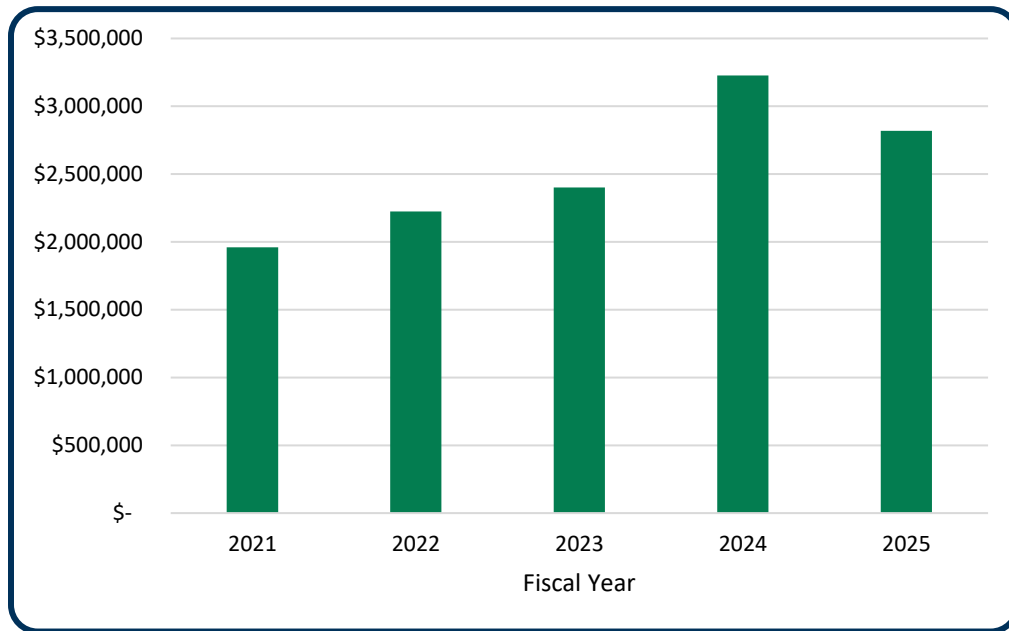
Division of Debt Collection

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. Collection fees decreased \$400,000 in fiscal year 2025, in part due to the decrease in the Division's workload of Department of Medical Assistance Services claims.

Debt Collection Fees

Chart 2



Source: Commonwealth accounting and financial reporting system

Below are additional details on the areas that we included in the current year's audit scope.

Grants Administration

The Office receives federal and state grants for funding related to a range of programs and areas of service totaling \$1.1 million in fiscal year 2025. The Office submits applications to federal and other state agencies and uses the funds to support its ongoing criminal and social justice-related programs in accordance with each grant agreement's terms.

Opioid Abatement Funds

The Opioid Abatement Fund is used to provide grants and loans to any agency of the Commonwealth or participating locality for the purposes established by § 2.2-2374 of the Code of Virginia. The funds come from settlements with opioid manufacturers or retailers. In fiscal year 2025, revenues in the fund totaled \$34.2 million, a decrease of \$38.3 million over the prior year. The Commonwealth began receiving opioid settlement funds in fiscal year 2022. The Commonwealth receives funds based on a planned schedule for each settlement. Fiscal year 2025 included eight sizable payments to the Office. The settlement funds pass through the Office to the Opioid Abatement Authority, which administers and distributes the funds to state agencies and localities. The Office transferred \$34.7 million in such funds to the Opioid Abatement Authority in fiscal year 2025.

The Commonwealth Opioid Abatement and Remediation (COAR) fund, new in fiscal year 2024, receives opioid settlement funds that are designated for opioid abatement or remediation, excluding

funds designated for transfer to the Opioid Abatement Authority or localities. The Office acts as the custodian of these funds and disburses them as appropriated. The Office transferred \$9.8 million in such funds from the Opioid Abatement fund to the COAR fund in fiscal year 2025. The Office transferred \$19.4 million in COAR funds to several state agencies during the fiscal year, including the Virginia Information Technologies Agency, Department of Health, Department of Criminal Justice Services, and the Virginia Foundation for Healthy Youth. The year-end balance of the COAR fund was \$50.8 million.

Federal Asset Forfeiture Fund

The Federal Asset Forfeiture Fund represents proceeds from the forfeiture of assets from drug cases. In fiscal year 2025, revenues in the fund totaled \$2.5 million, a sharp decrease from the prior year's \$32.7 million. The unusual amount of revenue received in the prior year is a result of the Federal Equitable Sharing Program. Under this program, state and local law enforcement agencies that participate in law enforcement efforts resulting in federal forfeitures can request an equitable share of the net proceeds from liquidated seized assets. The Office may only use funds received under this program to supplement, not replace, existing funding and for any purpose that supports the Office's mission. The funds are not earmarked for expenses related to asset forfeiture, crime reduction, or similar activities.



Staci A. Henshaw, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

August 12, 2026

The Honorable Jay Jones
Attorney General of Virginia

Joint Legislative Audit
and Review Commission

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, 2025. 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. We will follow up on findings not reviewed in a future audit.

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.

- Operational expenses
- Grant administration
- Legal services billings
- Opioid abatement funds
- Federal Asset Forfeiture Fund
- Settlement revenues and expenses
- Division of Debt Collection
- System access
- 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 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.

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 pertaining to information system security, 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 "Internal Control and Compliance Findings and Recommendations."

The Office has taken adequate corrective action with respect to select audit findings reported in the prior year that are listed as complete in the [Findings Summary](#) in this Appendix.

Exit Conference and Report Distribution

We discussed this report with management on October 5, 2026. 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

DBC/clj

Finding Title	Status of Corrective Action*	Fiscal Year First Reported
Independently Align the Information Security Officer	Complete	2022
Improve Threat Management and Incident Response Program	Ongoing	2025
Continue to Improve Virtual Private Network Security Controls	Ongoing	2019
Improve Server Operating System Security	Ongoing	2024
Develop and Implement a Process to Maintain Oversight Over Service Providers**	Ongoing	2022
Improve IT Risk Management and Contingency Process and Documentation**	Ongoing	2023

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

**We did not include these findings in the scope of our audit as per inquiry with management, we determined that corrective action was ongoing as of June 30, 2025.



COMMONWEALTH of VIRGINIA
Office of the Attorney General

Jay Jones
Attorney General

202 North 9th Street
Richmond, Virginia 23219
804-786-2071
FAX 804-786-1991
Virginia Relay Services
800-828-1120

October 9, 2026

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

Dear Ms. Henshaw:

We appreciate the Auditor of Public Accounts audit team for their professional approach and willingness to work with agency staff in the review of our Fiscal Year transactions and activities. The Office of the Attorney General consolidated our responses to the audit findings below.

Improve Threat Management and Incident Response Program

Type: Internal Control and Compliance

The Office does not ensure certain elements of its threat management and incident response program are conducted in accordance with the Commonwealth's Information Security Standard, SEC530 (Security Standard), as well as the Office's Information Security Program Policies (Office Policy) and Information Security Program Official Procedures (Office Procedures). Specifically, the following weaknesses exist:

1. The Office does not have an Incident Response Plan. Without a documented Incident Response Plan that includes all required elements, the Office may not consistently identify or respond to security incidents.
2. The Office does not designate an Information Security Incident Response Team for responding to cyber-attacks. The Office uses various tools and services for threat detection and monitoring but has not established a formal incident response team. Without establishing an Information Security Incident Response Team, the Office may not detect, contain, and recover from cyber incidents quickly and effectively.

3. During the fiscal year under review, the Office did not protect information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion. Not protecting information from intrusion monitoring tools presents increased risk of attackers altering monitoring data to mask or hide malicious actions, as well as loss of forensic evidence and investigative capability. As of July 2026, the Office added a file integrity monitoring service to protect information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion.
4. The Office does not consistently implement its documented process to track, prioritize, and categorize incidents in a service desk ticket. The Office's Information Technology (IT) Service Level Policy requires that the Office open a service desk ticket for service requests for all problems, including threats to data integrity or computer security. Ticketing systems provide structured workflows for prioritization, assignment, and resolution. Without consistently tracking information security incidents in its service desk ticketing system, the Office's response actions may be inconsistent, incomplete, or untracked, hindering rapid detection, analysis, and coordination across teams and increasing the time to resolve the incident.
5. The Office does not review and update the Office Policy and Office Procedures on an annual basis. Specifically, the Office has not reviewed and updated the Office Policy and Office Procedures since July 2023. As a result, the Office bases its information security policies and procedures on the Information Security Standard, SEC501, which is no longer valid. The Commonwealth's Information Security Standard, SEC530, superseded SEC501 as of March 2024. Without regularly reviewing and updating the Office Policies and Office Procedures, the Office may inconsistently implement the incident response program and increase the risk of mismanaging security incidents.
6. The Office does not adequately document procedures that detail its threat detection practices, logging and monitoring processes, incident handling practices, and mitigation measures used. By not documenting threat detection practices, monitoring and logging procedures, incident handling practices, and mitigation procedures, the Office increases the risk of not effectively detecting incidents and administrators not consistently monitoring and responding to potential security events.

The Office does not have a process to annually review and revise its Office Policy and Office Procedures, which led to the Office Policy and Office Procedures being out-of-date. In addition, the Office does not have an individual responsible for maintaining current information security policies and procedures. Further, turnover in the ISO role contributed to the Office not conducting certain elements of its threat management and incident response program in accordance with the Security Standard, Office Policy, and Office Procedures.

The Office should develop and document an Incident Response Plan that provides a roadmap for implementing all of the required elements. The Office should designate an Information Security Incident Response Team for responding to cyber-attacks; consistently implement its documented process to track, prioritize, categorize, and respond to incidents; and document its threat detection practices, logging and

monitoring processes, incident handling practices, and mitigation measures used. Finally, the Office should develop a process to annually review and update its Office Policy and Office Procedures, then review and update the Office Policy and Office Procedures to align with the requirements in the Security Standard. Improving the threat management and incident response program will help ensure the Office appropriately responds to malicious attempts to compromise confidentiality, integrity, and availability of sensitive information.

OAG Response

The OAG concurs with items 1 and 2 and will draft an Incident Response Plan, and the plan will identify an incident response team. The Incident Response Plan and related IT Security policies will be reviewed when standards change in the SEC 530 requirement standards or when changes in the environment require a review.

The OAG concurs with Item 3. OAG IT will identify the standard system logs required for monitoring and configure the newly enabled detection tools to alert potential malicious activity and improve controls to protect potential investigative related forensic data.

The OAG concurs with Item 4 that improvements need to be made by ensuring security incidents are consistently reported, tracked, prioritized, and categorized within the established ticketing system. The OAG will update the Service Desk SOP and associated policies, to ensure roles and responsibilities are identified and consistent within the documents. IT and Security team members will be trained and monitored according to the updates.

The OAG concurs with Items 5 and 6. Information security and IT will review; inventory, assign, and document the appropriate OAG policies aligned with SEC 530 and establish a process to monitor changes. Included in this review is a documented threat detection practice, processes and procedures for detecting and responding to incidents.

Continue to Improve Virtual Private Network Security Controls

Type: Internal Control and Compliance

First Reported: Fiscal Year 2019

The Office made progress since the prior year audit by resolving one of the two identified control weaknesses. However, the Office continues to not fully implement a required security control for its Virtual Private Network (VPN) in accordance with the Office Policy, as well as the Security Standard. We communicated one control weakness 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.

Not implementing all required security controls for the VPN increases the risk for a malicious user to exploit an existing vulnerability or weakness and cause a system compromise or unavailability. The Office's

previous employees did not appropriately implement the control. The Office has onboarded new employees and plans to resolve the identified weakness.

The Office should implement the security control mentioned in the FOIAE communication to ensure the VPN aligns with its Office Policy as well as the Security Standard. Implementing this control will help maintain the confidentiality, availability, and integrity of the Office's sensitive and mission critical data.

OAG Response

The OAG agrees that this security control had not been addressed during the last review period. This oversight has been corrected and will be ready to be marked as closed in the next review.

Improve Server Operating System Security

Type: Internal Control and Compliance

First Reported: Fiscal Year 2024

The Office made progress since the prior year audit by resolving one of the five identified control weaknesses. However, the Office continues to not implement certain controls and processes on the operating system that supports a sensitive Office server to properly secure the server in accordance with the Office Policy, the Office Procedures, the Security Standard, the Commonwealth's IT Risk Management Standard, SEC520 (Risk Management Standard), and industry best practices, such as the Center for Internet Security's Benchmark (CIS Benchmark). We identified and communicated four weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security mechanisms.

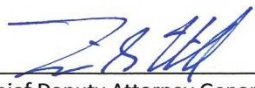
Lack of resources, personnel changes, and configuration errors by Office staff contributed to the issues. Without these controls, the Office may not effectively and consistently protect and mitigate risks to data.

The Office should ensure server operating system configurations, controls, and processes align with the requirements in the Office Policy, Office Procedures, the Security Standard, Risk Management Standard, and the CIS Benchmark. Implementing these controls will help maintain the confidentiality, integrity, and availability of the sensitive and mission critical data stored or processed on the server.

OAG Response

The OAG concurs with this finding and has successfully onboarded qualified full-time and contract staff that have started addressing these weaknesses.

Sincerely,



Chief Deputy Attorney General