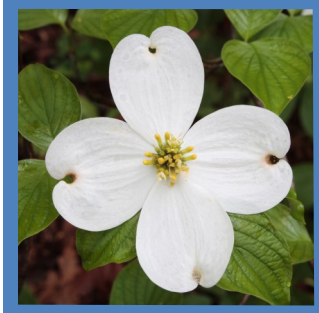


OFFICE OF THE EXECUTIVE SECRETARY OF THE SUPREME COURT OF VIRGINIA

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2023

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

AUDIT SUMMARY

We audited select internal controls over human resources and information technology processes for the judicial branch, which are the responsibility of the Office of the Executive Secretary (Executive Secretary) of the Supreme Court of Virginia, for the fiscal year ended June 30, 2023. Our primary focus regarding these processes was to review corrective actions taken by the Executive Secretary to address findings included in prior reports as reflected in the Audit Scope Overview and Findings Summary sections of this report. Our audit found:

- proper recording and reporting of all transactions, in all material respects, in the retirement benefits system;
- 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; and
- adequate corrective action with respect to three prior audit findings identified as complete in the Findings Summary.

The following entities of the judicial branch receive hiring and benefits processing (human resources) and information technology services from the Executive Secretary, particularly from the Department of Fiscal Services (Fiscal Services) and the Department of Judicial Information Technology (Judicial Technology), and as a result, they should consider the results of this audit:

- Circuit Courts
- Combined District Courts
- Court of Appeals of Virginia
- General District Courts
- Judicial Inquiry and Review Commission
- Juvenile and Domestic Relations District Courts
- Magistrate System
- Supreme Court of Virginia
- Virginia Criminal Sentencing Commission

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 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. Those corrective actions may include additional items beyond our recommendations.

We did not review management's corrective action on prior year findings identified as deferred in the Findings Summary included in the Appendix. We will follow up on these findings in a future audit.

-TABLE OF CONTENTS-

AUDIT FINDINGS AND RECOMMENDATIONS

Continue to Improve Sensitive Systems Risk Assessment and Contingency Planning Documentation
Type: Internal Control and Compliance
First Reported: Fiscal Year 2011

The Office of the Executive Secretary (Executive Secretary) continues to make progress in improving information technology (IT) risk management and contingency planning documentation. IT risk management and contingency planning documentation allows the Executive Secretary to appropriately consider business and system security risks when its IT environment undergoes major upgrades and/or significant changes.

Since our fiscal year 2019 audit, the Executive Secretary hired a full-time Information Security Officer (ISO) in September 2022, who developed a new template that combines a sensitive system's Risk Assessment and System Security Plan (SSP) template to align with the requirements in the Commonwealth's Information Security Standard, SEC501 (Security Standard). Additionally, the Executive Secretary resolved one of the prior year weaknesses by distributing a personnel security policy to staff assigned system security roles and has made some progress with the remaining five weaknesses outlined below.

- The Executive Secretary partially completed one SSP for its 56 sensitive systems. The Security Standard requires the Executive Secretary to conduct a risk assessment at least once every three years, conduct annual self-assessments to determine the continued validity of the risk assessment, and prepare a report of each risk assessment that includes, at a minimum:

    - Identification of all vulnerabilities discovered during the assessment and

    - An executive summary of major findings and risk mitigation recommendations.

The Security Standard also requires the Executive Secretary to develop an SSP for the information system and review it on an annual basis or more frequently if required to address an environmental change (*Security Standard, sections: 6.2 Risk Assessment, PL-2 System Security Plan*).

- The Executive Secretary's SSP template includes a section to determine whether each type of data is subject to regulatory requirements, but the Executive Secretary has not completed this section for its 56 sensitive systems. Regulatory requirements include, but are not limited to, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Internal Revenue Service (IRS) Publication 1075, Payment Card Industry (PCI), and Federal National Security Standard requirements (*Security Standard, section: 4.2.2 – IT System and Data Sensitivity Classification*).

- The Executive Secretary does not include a review of its Continuity of Operations Plan's (COOP) activation procedures and IT disaster recovery components during monthly tabletop

exercises. The Security Standard requires the Executive Secretary to conduct an exercise annually, or more often as necessary, of the COOP's IT disaster recovery components to assess their adequacy and effectiveness and require a review and revision of those components following the exercise (*Security Standard, sections: CP-1-COV-1 Contingency Planning Policy and Procedures, CP-4 Contingency Plan Testing and Exercises*).

- The Executive Secretary does not perform a full recovery and reconstitution of an information system to a known state as part of its contingency testing (*Security Standard, section CP-4-CE-4 Contingency Plan Testing and Exercises*).

- The Executive Secretary created its SSP template with plans to document restoration requirements (hardware, software, and configurations) for sensitive systems; however, the Executive Secretary has not completed this documentation for its 56 sensitive systems as required by the Security Standard (*Security Standard, section: CP-2 Contingency Plan*).

By having outdated risk management documentation, the Executive Secretary cannot accurately determine which information security controls to implement. This deficiency in documentation may result in the Executive Secretary spending too many resources on insignificant controls or not having enough controls to protect sensitive information. Furthermore, by not reviewing COOP activation procedures or conducting a full system recovery test as part of its periodic COOP and DRP testing, the Executive Secretary, and the other entities for which it provides IT services may experience significant delays in meeting recovery time objectives for restoring sensitive systems and essential business functions in the event of an emergency or disaster.

In January 2020, the Executive Secretary hired its Department of Judicial Information Technology (Judicial Technology) Director and then shortly thereafter, in March, the COVID-19 pandemic resulted in major changes in the Executive Secretary's operations. The pandemic shifted the Executive Secretary's priorities to ensure operations could continue under the health guidelines at the time, delaying the Executive Secretary's corrective action progress to improve its risk management and contingency planning documentation. Additionally, the new ISO determined the sensitive systems list and 26 risk assessments previously completed were incomplete and outdated as of the 2021 calendar year, causing the Executive Secretary to revise and extend its timeline for corrective action.

The Executive Secretary should continue its efforts to improve its risk management and contingency planning documentation to ensure the information reflects the current environment and addresses the weaknesses described above. Additionally, the Executive Secretary should dedicate the necessary resources to ensure it tests its COOP's procedures and the full recovery and reconstitution of an IT system.

Maintain Oversight of Third-Party Service Providers
Type: Internal Control and Compliance
First Reported: Fiscal Year 2016

The Executive Secretary continues not to have a complete formal process for how it is to use System and Organization Control (SOC) reports to maintain oversight of third-party service providers (providers). Providers are entities that perform outsourced functions on behalf of the Commonwealth, which could be either IT and/or fiscal-related. While the Executive Secretary has made improvements in this area since our fiscal year 2021 audit, the Executive Secretary's policies and procedures do not include requirements or actions for staff to review and document their analysis of SOC reports for the Executive Secretary's IT and fiscal providers.

For IT services, the Security Standard and the Commonwealth's Hosted Environment Information Security Standard, SEC525 (Hosted Environment Security Standard), state, management remains accountable for maintaining compliance with the Security Standard and Hosted Environment Security Standard through documented agreements with providers and oversight of services provided. Additionally, the Hosted Environment Security Standard requires the Executive Secretary to develop, document, and implement appropriate system and services acquisition policies and procedures including, but not limited to, its process to review an annual audit report of the provider's environment conducted by an independent audit firm (*Security Standard, section: 1.1 Intent; Hosted Environment Security Standard, sections: 1.1 Intent, SA-1 System and Services Acquisition Policy and Procedures, SA-9 External Information System Services*). Additionally, the Commonwealth Accounting Policies and Procedures (CAPP) Manual, which the Executive Secretary adopts, Topic 10305 - Internal Control, contains similar control activities over providers that perform significant fiscal processes.

Without a formally documented policy and procedure to obtain and document its analysis of independent audit assurance over providers' internal controls, the Executive Secretary cannot consistently validate that its providers have effective controls to protect its mission-critical and confidential data and ensure the integrity of fiscal processes. While the Executive Secretary developed a formal policy for providers to implement specific IT security and fiscal controls, the Executive Secretary did not include requirements for its oversight process. The Executive Secretary also prioritized implementing corrective actions to resolve other prior audit findings to improve its IT security posture.

The Executive Secretary should develop a formal policy and procedure that reflects its process for identifying providers and gaining appropriate assurance over outsourced functions, including providers whose services affect the fiscal operations of the Executive Secretary. The Executive Secretary should also ensure its formal policy and procedure aligns with the Hosted Environment Security Standard's requirements and CAPP Manual expectations for maintaining oversight of its providers. To uphold consistency and continuity in maintaining oversight of both IT and fiscal providers, the Executive Secretary should ensure its policies and procedures includes a standard approach for staff to document their final decisions and any actions taken by the Executive Secretary that result from the assurance report evaluation process.

Conduct and Document a Risk Assessment for Disaster Recovery Site
Type: Internal Control and Compliance

The Executive Secretary does not conduct and document an analysis of risks for its disaster recovery site. A disaster recovery site is an alternate off-site location used to restore, in a timely manner, IT systems supporting mission-essential business functions in the event the main data center becomes unavailable. We communicated the specific risks 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.

Without conducting and documenting a risk assessment to assess the potential threats to the disaster recovery site, the Executive Secretary may not identify and implement mitigating controls to reduce the risk to a level acceptable by management. Limited funding and the Executive Secretary prioritizing implementing corrective actions to resolve other prior audit findings to improve its security posture led to the Executive Secretary not conducting and documenting a risk assessment.

The Executive Secretary should conduct and document a risk analysis of its disaster recovery site to assess the potential vulnerabilities and threats as discussed in the FOIAE document. As part of its risk analysis, the Executive Secretary should document the compensating security controls that reduce the likelihood and magnitude of the risks identified to a level acceptable by management.

Properly Complete and Retain Employment Eligibility Forms
Type: Internal Control and Compliance
First Reported: Fiscal Year 2021

The Executive Secretary continues to not consistently complete Employment Eligibility Verification (I-9) forms in accordance with guidance issued by the U.S. Citizenship and Immigration Services of the U.S. Department of Homeland Security. The Executive Secretary did not retain required documentation as evidence that it completed employment eligibility determination at the time of onboarding for six out of 40 employees (15%) tested. Of these six employees, the Executive Secretary could not provide any of the required documentation for two of the employees and in the documentation for the remaining four employees, Section 2 of the I-9 form was either missing entirely or left substantially blank. Additionally, excluding the six employees with missing documentation, the Executive Secretary did not retain documentation for 24 out of the 34 remaining employees (71%) tested, showing that staff completed the E-Verify process in a timely manner. Collectively, of the 40 new hires randomly tested for the entities that rely on the services of the Executive Secretary, as listed in the Audit Summary, staff correctly completed and retained only 10 (25%) of their I-9 forms.

The Immigration Reform and Control Act of 1986 requires that employers complete the I-9 form to verify both identity and employment eligibility for all employees. The U.S. Citizenship and Immigration Services set forth federal requirements for completing the I-9 form in the Handbook for Employers M-274 (Handbook). Chapter 9 of the Handbook requires employers to retain a completed I-9 form on file for each employee. The completed I-9 form must be kept as long as the employee works for the employer, and for a certain amount of time after they stop working. Chapter 3 of the Handbook requires

that entities properly complete all parts of Section 1. Chapter 4 requires the employer to complete Section 2 and ensure that it matches the employee information in Section 1 of the I-9 form. Additionally, Chapter 3 also requires the employee to complete and sign Section 1 of the I-9 form by the first date of employment. Noncompliance with federal regulations related to employment verification could result in civil and/or criminal penalties and debarment from government contracts.

The Executive Secretary's policies and procedures governing employment eligibility do not address several important factors including: who should perform each function, when to perform those functions, and how to retain documentation of the procedures performed. Additionally, the Executive Secretary's previous corrective action of implementing internal reviews to monitor and evaluate the presence and function of related controls were not effective in ensuring staff completed I-9 forms and retained documentation in accordance with the Handbook. The Executive Secretary should ensure its staff complete I-9 forms and retain documentation as required. The Executive Secretary should also update policies and procedures to ensure staff are aware of their roles and responsibilities pertaining to completion of I-9 forms. Additionally, since the Executive Secretary has implemented procedural, training, and staffing updates throughout fiscal years 2022 and 2023, the Executive Secretary should continue to review and revise these procedures to ensure their effectiveness.

Remove Access to the Retirement Benefits System Timely

Type: Internal Control and Compliance

The Executive Secretary does not have adequate controls in place to ensure that staff remove access to the Commonwealth's retirement benefits system timely. Fiscal Services did not remove access timely, within 24 hours, for four of the thirteen (31%) employees who separated from the agency or transferred internally to roles that no longer required access to the system. Instead, Fiscal Services removed access between two and six days after the employees no longer required access.

The Security Standard, Section PS-4, states an organization must disable information system access within 24 hours of employee separation and terminate any authenticators or credentials associated with the individual. Additionally, Section PS-5, requires an organization to modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer of personnel within the organization. Untimely termination of access increases the risk of unauthorized use of the system which could result in unauthorized changes that could impair data integrity.

Fiscal Services indicated that managers in Human Resources did not inform them in a timely manner of staff separations within Human Resources, causing the access removal to occur outside of the Security Standard requirements. The Executive Secretary should ensure that managers responsible for reporting terminations and transfers notify Fiscal Services in a timely manner so that removal of access can occur within the 24-hour Security Standard requirement.

AUDIT SCOPE OVERVIEW

There are 31 Magistrate Offices, 120 Circuit Courts, 41 Combined District Courts, 83 Juvenile and Domestic Relations District Courts, and 86 General District Courts. Within these offices and courts, there were over 3 million cases filed during calendar year 2023 ranging from traffic violations and simple civil suits to major felonies.

The Chief Justice of the Supreme Court serves as the head of the judicial branch. The court system, the magistrate system, and various judicial agencies comprise the judicial branch of government. The Executive Secretary aids the Chief Justice in this mission by providing administrative services to the judicial branch, which has approximately 2,900 employees. The Executive Secretary consists of the following ten departments:

- Assistant Executive Secretary and Counsel
- Court Improvement Program
- Educational Services
- Fiscal Services
- Human Resources
- Judicial Information Technology
- Judicial Planning
- Judicial Services
- Legal Research
- Legislative and Public Relations

Our audit focused on human resource services, primarily related to reviewing corrective actions taken by the Executive Secretary to address findings included in prior reports. The Fiscal Services and Human Resources departments implement internal controls and records and report payroll and benefits for all judicial agencies, except for clerks of the circuit courts and their direct staff. During the current audit, we tested retirement benefits system access, reconciliations, and census data recording for the various judicial agencies as well as the employment eligibility verification process.

Judicial Technology serves as the information technology service provider to the judicial branch agencies, managing IT systems and projects for all judicial agencies. During our audit we reviewed corrective actions taken to address selected prior findings related to general IT controls surrounding information system security.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

July 26, 2024

The Honorable S. Bernard Goodwyn
Chief Justice, Supreme Court of Virginia

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

We have audited select human resources and information technology internal control processes of the **Office of the Executive Secretary (Executive Secretary) of the Supreme Court of Virginia** for the year ended June 30, 2023. 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 with regard to human resources and information technology internal control processes were to evaluate the accuracy of transactions in the retirement benefits system; review the adequacy of the Executive Secretary's internal controls; and test compliance with applicable laws, regulations, contracts, and grant agreements. We also reviewed corrective actions for select 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

Management of the Executive Secretary 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, as they relate to the audit objectives, sufficient to plan the audit. We considered significance and risk in determining the nature and extent of our audit procedures. We performed audit tests to determine whether the Executive Secretary'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 as they pertain to our audit objectives.

Our audit procedures included inquiries of appropriate personnel, inspection of documents, records, and contracts, and observation of the Executive Secretary's operations. We 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 Executive Secretary properly stated, in all material respects, transactions recorded and reported in the Commonwealth's retirement benefits system, relating to the audit objectives.

We noted certain matters involving select human resources and information technology internal control processes and their 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 entitled "Audit Findings and Recommendations."

The Executive Secretary has taken adequate corrective action with respect to the audit findings reported in the prior year that are listed as complete in the Findings Summary in the Appendix.

Exit Conference and Report Distribution

We provided a draft of the report for review on July 30, 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 Chief Justice, Governor, and General Assembly, management, and citizens of the Commonwealth of Virginia and is a public record.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

GDS/ clj

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	First Reported for Fiscal Year
Obtain and Retain an Information Security Officer	Complete	2016
Improve Retirement Benefits System Reconciliation Documentation and Procedures	Complete	2018
Continue Performing a Risk Analysis for Exceptions to the Acceptable Use Policy	Complete	2019
Improve Disaster Recovery Controls	Complete	2019
Continue to Improve Sensitive Systems Risk Assessment and Contingency Planning Documentation	Ongoing	2011
Maintain Oversight of Third-Party Service Providers	Ongoing	2016
Conduct and Document a Risk Assessment for Disaster Recovery Site	Ongoing	2023
Properly Complete and Retain Employment Eligibility Forms	Ongoing	2021
Remove Access to the Retirement Benefits System Timely	Ongoing	2023
Continue Improving Intangible Capital Assets Expense Tracking and Reporting	Deferred	2007
Perform Information Technology Security Audits	Deferred	2019

* A status of **Complete** indicates adequate corrective action taken by management. A status of **Ongoing** indicates new and/or existing findings that require management's corrective action as of fiscal year end. A status of **Deferred** indicates that we will follow-up in a future audit when management asserts that it has taken adequate corrective action; per inquiry with management, we determined that corrective action was ongoing as of June 30, 2023 for these findings.

EXECUTIVE SECRETARY
KARL R. HADE

ASSISTANT EXECUTIVE SECRETARY & LEGAL COUNSEL
EDWARD M. MACON

COURT IMPROVEMENT PROGRAM
SANDRA L. KARISON, DIRECTOR

EDUCATIONAL SERVICES
CAROLINE E. KIRKPATRICK, DIRECTOR

FISCAL SERVICES
BARRY M. WENZIG, DIRECTOR

HUMAN RESOURCES
RENÉE FLEMING MILLS, DIRECTOR

SUPREME COURT OF VIRGINIA

JUDICIAL INFORMATION TECHNOLOGY
MICHAEL J. RIGGS, SR., DIRECTOR

JUDICIAL SERVICES
PAUL F. DELOSH, DIRECTOR

LEGAL RESEARCH
STEVEN L. DALLE MURA, DIRECTOR

LEGISLATIVE & PUBLIC RELATIONS
ALISA W. PADDEN, DIRECTOR

MAGISTRATE SERVICES
JONATHAN E. GREEN, DIRECTOR

OFFICE OF THE EXECUTIVE SECRETARY
100 NORTH NINTH STREET
RICHMOND, VIRGINIA 23219-2334
(804) 786-6455

August 16, 2024

Ms. Stacy A. Henshaw, CPA
Auditor of Public Accounts
James Monroe Building
101 North 14th Street 8th Floor
Richmond, VA 23219

Dear Ms. Henshaw:

Thank you for providing the Office of the Executive Secretary of the Supreme Court of Virginia the opportunity to review the Audit Findings and Recommendations that are being considered for inclusion in the audit report The Office of the Executive Secretary (OES) takes internal controls and compliance very seriously and strives to maintain reasonable assurance of the integrity of all fiscal, administrative and information technology processes. The following items were communicated in the audit draft report on July 26, 2024 and our responses are listed below:

Properly Complete and Retain Employment Eligibility Forms

Human Resources will continue to review and update policies and procedures regarding employee eligibility forms, including roles and responsibilities that are responsible for each function. Although controls such as new hire checklists and webinars are currently in place, we will continue to review and assess internal processes to ensure that employee eligibility forms are received timely and accurately. Additional staff training will be implemented and procedures will be updated to ensure that document retention deficiencies are remediated and management of the entire employee eligibility process is improved.

Remove Access to the Retirement Benefits System Timely

Human Resources will continue to work with Fiscal Services to ensure procedures are clarified and updated regarding the removal of access to the retirement benefits system. The Commonwealth's Information Security Standard requirements regarding system access removal

have been reviewed and management will ensure access is removed within 24 hours of employee separation.

Continue to Improve Sensitive Systems Risk Assessment and Contingency Planning Documentation

The Information Security Officer (ISO) has established new processes, templates, and a schedule to address the assessment of risk for the Executive Secretary's sensitive systems. These will be used to focus efforts towards completing a System Security Plan for each of the 56 IT systems that have been identified as sensitive. The ISO will continue to focus efforts towards making improvements related to Contingency Planning documentation, to include a more formal documentation of annual exercises related to the activation of the Contingency Plan.

Maintain Oversight of Third-Party Service Providers

As noted, the Executive Secretary has made significant improvements in its third-party service provider oversight program to include the annual review of provider's security reports. Additional specific concerns have been noted and the ISO will update processes, including documenting a formal procedure for the review of service provider's security reports, to make further improvements in this area of the agency's information security program.

Conduct and Document a Risk Assessment for Disaster Recovery Site

While the Executive Secretary has a Disaster Recovery Site to provide redundancy in the event of a disaster, budget constraints remain a significant limiting factor for Executive Secretary to address all concerns noted in the FOIA exempt findings related to the existing Disaster Recovery setup. The ISO and others within the Office of Executive Secretary will work towards formally documenting an assessment of risks related to the Executive Secretary's Disaster Recovery Site.

With best wishes, I am

Very truly yours,

KRH

Karl R. Hade