



OFFICE OF THE EXECUTIVE SECRETARY
OF THE
SUPREME COURT OF VIRGINIA

REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2019

Auditor of Public Accounts
Martha S. Mavredes, CPA
www.apa.virginia.gov
(804) 225-3350



AUDIT SUMMARY

We audited the retirement benefits system and information system security control 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, 2019. We also audited the agreements governing the administrative services the Executive Secretary provides to the Judicial Branch. In addition, we performed analytical procedures over select revenue and expense activity as detailed in the Audit Scope Overview Section. Our audit found:

- proper recording and reporting of transactions, in all material respects, in the Commonwealth's accounting and financial reporting and retirement benefits system, relating to the audit objectives, except as noted in the finding titled "Improve Documentation and Review of Retirement Benefits System Reconciliation" in the section entitled "Status of Prior Year Audit Findings";
- matters involving internal control and its operation related to the retirement benefits system, information system security, and administrative services agreements necessary to bring to management's attention; and
- adequate corrective action with respect to the prior audit finding identified as resolved in the [Findings Summary](#) in the Appendix.

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

The following entities of the Judicial Branch receive payroll, information technology, and general administrative services from the Executive Secretary, particularly from its department of Fiscal Services (Fiscal) 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

- TABLE OF CONTENTS -

	<u>Pages</u>
AUDIT SUMMARY	
STATUS OF PRIOR YEAR AUDIT FINDINGS	1-5
AUDIT SCOPE OVERVIEW	6-10
INDEPENDENT AUDITOR'S REPORT	11-13
APPENDIX: FINDINGS SUMMARY	14
AGENCY RESPONSE	15-17
AGENCY OFFICIALS	18

STATUS OF PRIOR YEAR AUDIT FINDINGS

Information Systems

Obtain and Retain an Information Security Officer

Type: Internal Control and Compliance

Repeat: Yes (First Issued in 2016)

The Executive Secretary has not employed an Information Security Officer (ISO) to improve and maintain its information security program. The lack of an ISO contributed to the continuance of other weaknesses, as noted below.

The Commonwealth's Information Security Standard, SEC 501 (Security Standard), Section 2.4, requires the agency head to designate an ISO that is responsible for developing and managing the information security program. Additionally, the Security Standard requires the Executive Secretary to implement several security controls to safeguard sensitive and mission critical data that is stored in the information technology (IT) environment. The lack of an ISO reduces the ability to effectively improve the Executive Secretary's security posture and resolve the weaknesses discussed in the separate recommendations. This increases the risk of not protecting the confidentiality, integrity, and availability of sensitive Commonwealth information. The Executive Secretary should continue efforts to obtain and retain a qualified ISO.

Continue to Improve Sensitive Systems Risk Assessment and Contingency Planning Documentation

Type: Internal Control and Compliance

Repeat: Yes (First Issued in 2011)

The Executive Secretary continues to make progress in improving IT risk management and contingency planning documentation. The 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 material changes. Since the audit conducted for fiscal year 2016, the Executive Secretary hired an external firm to assist in improving the information security program, including the IT risk management and contingency planning program. One weakness is resolved, and significant progress is evident in corrective actions for two of the seven total weaknesses identified. However, six weaknesses related to IT risk management and contingency requirements as set forth in the Security Standard continue to be unresolved. The details of these control weaknesses have been communicated 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 its sensitivity and description of security controls.

By having outdated risk management and contingency planning documentation, the Executive Secretary cannot accurately determine which information security controls to implement. This may result in the Executive Secretary spending too many resources on insignificant controls or not having enough controls to protect sensitive information. As a result, the Executive Secretary may not be able to recover its essential business functions and IT systems in a timely manner to meet its recovery time

objectives. The Executive Secretary should continue to improve its risk management and contingency planning documentation to ensure the information reflects the current environment and addresses the weaknesses described in the FOIAE communication.

Improve Disaster Recovery Controls

Type: Internal Control and Compliance

Repeat: Yes (First Issued in 2016)

The Executive Secretary has not made significant progress in improving certain critical disaster recovery controls. Without certain disaster recovery controls, the Executive Secretary is putting the Commonwealth's judicial branch at risk for the disruption of performing its mission-essential business functions, which includes interpreting and administering the Commonwealth's laws and resolving legal conflicts. Since the audit conducted in 2016, the Executive Secretary has focused its efforts on higher priorities and researching disaster recovery solutions. The Executive Secretary cites lack of necessary resources as the cause for lack of progress in resolving these control weaknesses.

The Executive Secretary should obtain the necessary resources to improve its disaster recovery controls described in the FOIAE communication. This will reduce the risk of disruption to the judicial branch in the performance of its mission-essential functions and ensure that the Executive Secretary can restore systems and applications per its own expectations.

Maintain Oversight of Third-Party Service Providers

Type: Internal Control and Compliance

Repeat: Yes (First Issued in 2016)

The Executive Secretary has not established a process to maintain oversight over third-party service providers (Providers). Providers are entities that perform outsourced tasks or functions on behalf of the Commonwealth.

The Security Standard, Section 1.1, states management remains accountable for maintaining compliance with the Security Standard through documented agreements with providers and oversight of services provided. Additionally, the Commonwealth's Hosted Environment Information Security Standard, SEC 525 (Hosted Environment Security Standard), Section SA-1, requires the Executive Secretary to develop, document, and implement appropriate system and services acquisition policies and procedures. Also, SA-9-COV-3 of the Hosted Environment Security Standard requires the Executive Secretary perform an annual security audit or review the annual audit report of the provider's environment conducted by an independent audit firm.

Without a documented and established process to identify providers and gain assurance over providers' internal controls, the Executive Secretary cannot consistently validate that those providers have effective security controls to protect its mission critical and confidential data. The Executive Secretary should develop and implement a formal framework for identifying providers and gaining appropriate assurance over outsourced operations that affects its IT environment, sensitive data, or mission-critical processes. This process should include developing formal policies and procedures to

maintain a list of all providers and obtaining independent audit assurance for the Executive Secretary's evaluation. To maintain consistency and continuity, the Executive Secretary should also develop and implement procedures for documenting final decisions and action items that come as a result of the assurance report evaluation process.

Perform Information Technology Security Audits

Type: Internal Control

Repeat: Yes (First Issued in 2016)

The Executive Secretary does not perform security audits over its IT systems classified as sensitive on a periodic basis. Currently, there are 29 sensitive systems identified in the risk management and contingency planning documentation, and not all the control areas for all systems have received the necessary independent security audit. The performance of IT security audits ensures that sensitive systems are configured and maintained in compliance with internal policies and procedures, the Security Standard, and industry best practices. Lack of periodic IT security audits on sensitive systems, increases the risk for sensitive system vulnerabilities and undetected threats within the systems' configuration settings and system management processes. This also increases the risk for malicious users to exploit those vulnerabilities to compromise sensitive information and render systems unavailable.

The Executive Secretary should develop and maintain an IT security audit plan to schedule all sensitive systems audits on a periodic basis.

Continue Performing a Risk Analysis for Exceptions to the Acceptable Use Policy

Type: Internal Control and Compliance

Repeat: Yes (First Issued in 2016)

The Executive Secretary does not perform a risk analysis for exceptions made to certain information security policies and controls. The implemented Acceptable Use Policy prohibits the use of computer or network resource to access pornography, gaming sites or audio/video entertainment for non-business purposes. However, the policy excludes executive-level personnel and magistrates such as Justices of the Supreme Court of Virginia, Judges of the Court of Appeals of Virginia, circuit court clerks, and internal Directors and there is no documentation of the risk analysis for this exception. Since the prior audit the Executive Secretary has drafted several revisions to the policy to remove the broad exceptions but has not obtained final approval for the policy.

The Security Standard, Section RA-3, requires a risk assessment evaluating the likelihood and magnitude of unauthorized access, use, disclosure, modification, or destruction of the information system. Per the requirement, the Executive Secretary should document and review the risk assessment on an annual basis or more frequently as needed, and distribute to appropriate personnel, such as management.

Not performing and documenting a risk analysis results in the inability to ensure that any compensating controls adequately mitigate the risks presented by allowing exceptions to this policy. The Executive Secretary should perform a risk analysis for providing certain employees with an exception to

the Acceptable Use Policy. The analysis should include risks created by the granting of the exceptions, the controls that mitigate the risks, and management's decision to accept any residual risks or to implement additional controls.

Other Areas

Establish Memoranda of Understanding with Separate Agencies

Type: Internal Control

Repeat: Yes (First Issued in 2018)

As noted in our prior audit, the Executive Secretary does not have formal Memoranda of Understanding with the separate agencies for which it provides administrative and payroll services. These agencies include the Judicial Inquiry and Review Commission and the Virginia Criminal Sentencing Commission. The Executive Secretary relies on the Organization and Functions Manual (Manual) by the Office of the Executive Secretary to establish the role of and services provided; however, this Manual is an internal document and is not distributed among and approved by these other agencies.

As a best practice, Memoranda of Understanding should be established between agencies performing or receiving services from other agencies in order to lay out the terms of services provided, the responsibilities of each of the agencies involved, and the funding sources for these services. The lack of these Memoranda could result in misunderstandings of agencies' responsibilities related to important processes which can lead to the breakdown of crucial controls. This could potentially result in the key processes being done ineffectively or not at all. Memoranda can also help to avoid misunderstandings related to budget and funding sources between agencies. Management indicated in our prior audit that they did not realize that the Memoranda were necessary. Due to numerous administrative issues in both the Supreme Court and the noted agencies, the process of establishing these documents has not been undertaken.

Supreme Court should continue to attempt to establish a Memorandum of Understanding with each of the separate agencies in order to document Supreme Court's responsibilities under the arrangement and funding for those services.

Improve Documentation and Review of Retirement Benefits System Reconciliations

Type: Internal Control

Repeat: Yes (First Issued in 2018)

Prior Title: Improve Retirement Benefits System Reconciliation Documentation and Procedures

As noted, our prior audit, the Executive Secretary does not retain monthly reconciliations between the agency's human resources (HR) system and the Commonwealth's retirement benefits system. Although existing policies and procedures detail the reconciliation process, they do not specify requirements to document the reconciliation and results. The lack of documentation of reconciliation and review resulted in improper entry of employee information into the system. For two of nine newly enrolled employees, incorrect spelling of employee names was entered. For one of nine terminated employees, the employee start and/or end date was incorrect.

The Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic 50410 recommends performing a monthly reconciliation of the agency's HR system to the retirement benefits system to ensure proper calculation of the creditable compensation, and that employees are reported in the proper retirement plan codes. As a best practice, Supreme Court should maintain employee enrollment information and supporting documentation to ensure changes are properly entered and accurate. Incorrect data can lead to improper confirmation of retirement contributions, affecting employee retirement calculations.

Supreme Court should expand its currently documented procedures to include appropriate reconciliation documentation. In addition, Supreme Court should develop a process to ensure proper review is performed when entering employee data into the system to minimize keying errors.

AUDIT SCOPE OVERVIEW

There are 120 Circuit Courts in the 31 judicial circuits of Virginia. There are 124 General District and 122 Juvenile and Domestic Relations courts in Virginia's 32 judicial districts. Within these courts there are over 4 million cases filed per year ranging from traffic violations to simple civil suits to major felonies.

The Chief Justice of the Supreme Court serves as the head of the Judicial Branch. The Judicial Branch of government is composed of the court system, the magistrate system, and various judicial agencies. The Executive Secretary aids the Chief Justice in this mission by providing administrative services to the Judicial Branch. 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

Fiscal serves as the payroll administrator for the Judicial Branch. Fiscal, along with Human Resources, implements controls and records and reports payroll and benefits for all judicial agencies, with the exception of clerks of the circuit courts and their direct staff. This included over 3,700 salaried and wage employees in the fiscal year ending June 30, 2019. We tested the following areas as part of our audit:

- Retirement benefits system access, reconciliations, and data recording

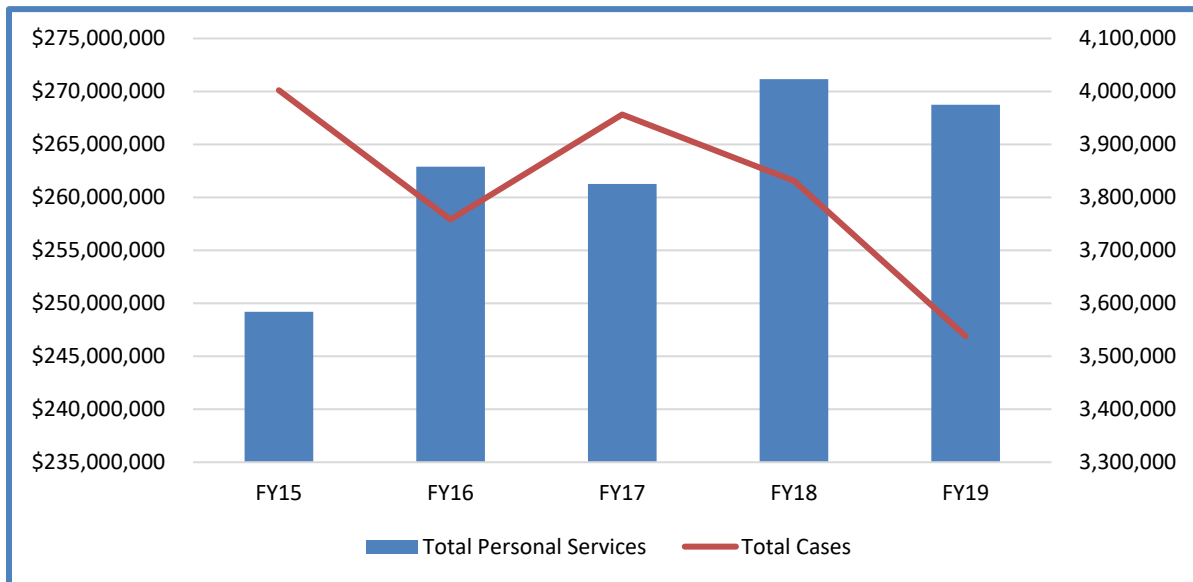
Judicial Information Technology serves as the information technology (IT) service provider to the Judicial Branch, managing IT systems and projects for all judicial agencies. Based on the management recommendations from prior audits, we determined information systems security at the Executive Secretary was a potential risk.

We performed an analytical review over a five-year period (2015 through 2019) to determine if there were any areas of revenues and expenses or transactions of specific judicial agencies that might be more at risk. Our overall expectation was that revenues and expenses, in general, would fluctuate from year to year in correlation with the number of court cases filed in each court each year. However, our expectation with respect to payroll expenses and personal services was that these expenses would not fluctuate based on court cases but would only change in years where there were statewide increases in salary or benefit expenses. The results of our analytical review are noted below.

Our expectation for payroll expenses was met and these did not change by any significant amount as court filings fluctuated. We determined that regardless of the number of cases filed, payroll expenses did not fluctuate except in years where a statewide payroll increase was granted (2 percent in fiscal year 2016, and 3 percent in 2018), or if benefit expenses increased. The results of our payroll review can be seen in Chart 1 below.

Personal Services – All Judicial Agencies

Chart 1

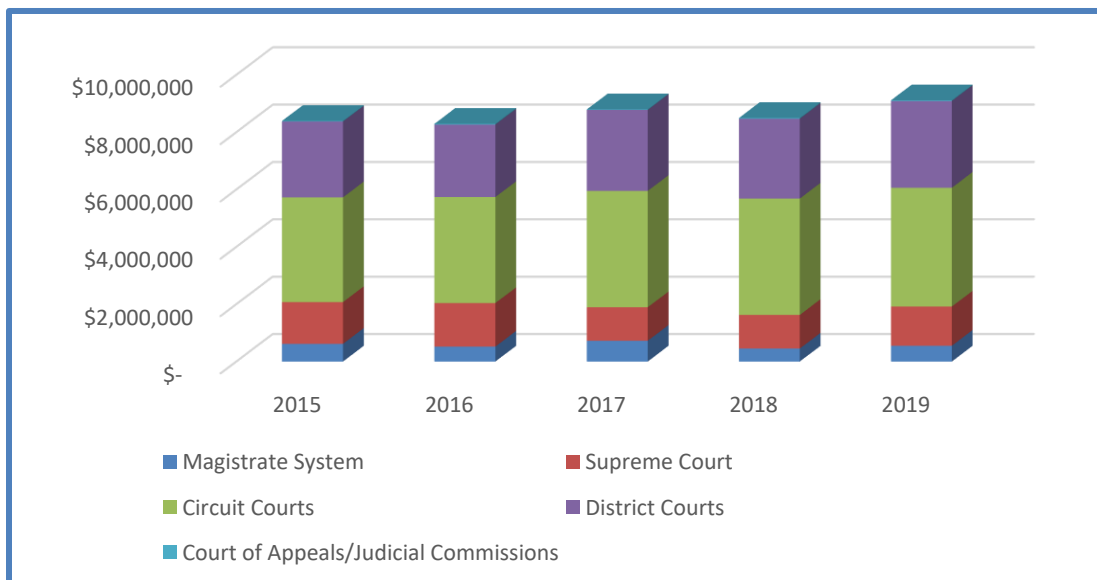


Source: Commonwealth's accounting and reporting system

An additional area of focus was travel expenses. Traditionally, the Judicial system is one of the top areas for travel spending due to activities in the criminal and involuntary mental commitment areas. Travel expenses for the Judicial system in total average between \$8 million and \$9 million per year. The most significant travel expenses are for personal vehicles and custodial care, primarily extradition expenses. Chart 2 provides an overview of all travel by Judicial agency.

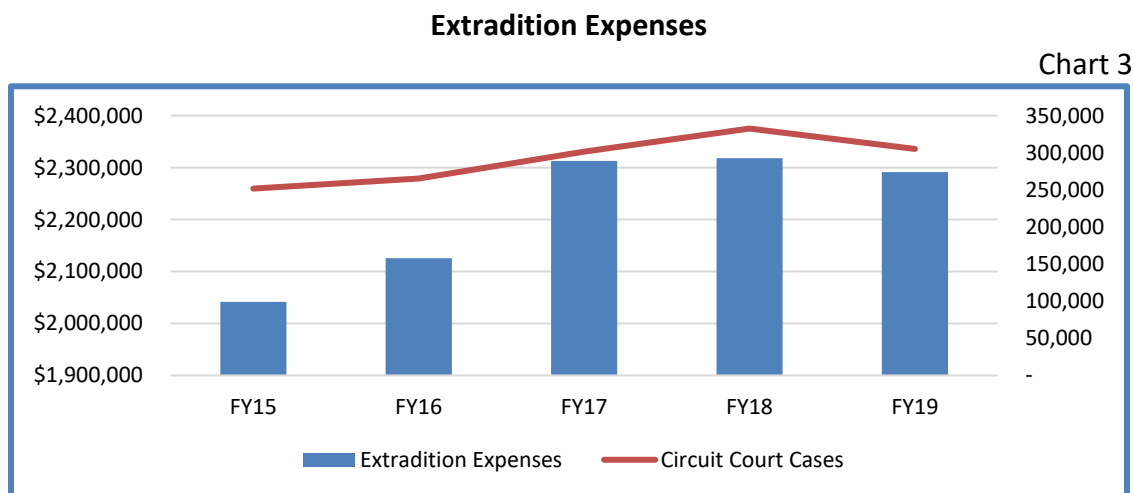
Travel Expenses by Judicial Agency

Chart 2



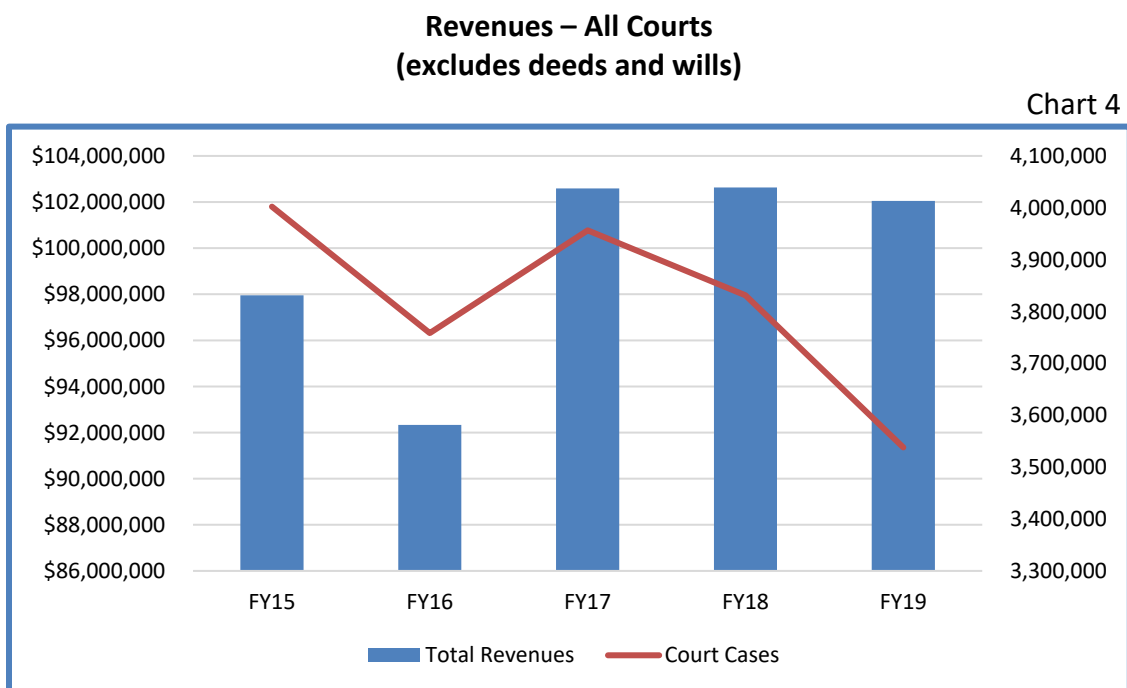
Source: Commonwealth's accounting and reporting system

There is no direct correlation between the number of cases filed and the amount of travel expenses in a given year. However, extradition expenses which are primarily incurred by the Circuit Courts appear to have some correlation to filed cases. These are expenses paid to extradite persons facing criminal charges from other states and/or countries to Virginia for trial. These expenses vary widely dependent on the type of case, distance of travel, and mode of travel. Chart 3 outlines the five-year trend for extradition expenses.



Source: Commonwealth's accounting and reporting system

While overall, expenses do not appear to correlate directly to the number of court cases filed, this does not hold true for revenues of individual courts. Chart 4 illustrates that while the revenues can vary depending on the types of cases filed within a particular year, looking at the Courts system as a whole, there does not appear to be a relationship between revenues and cases filed.

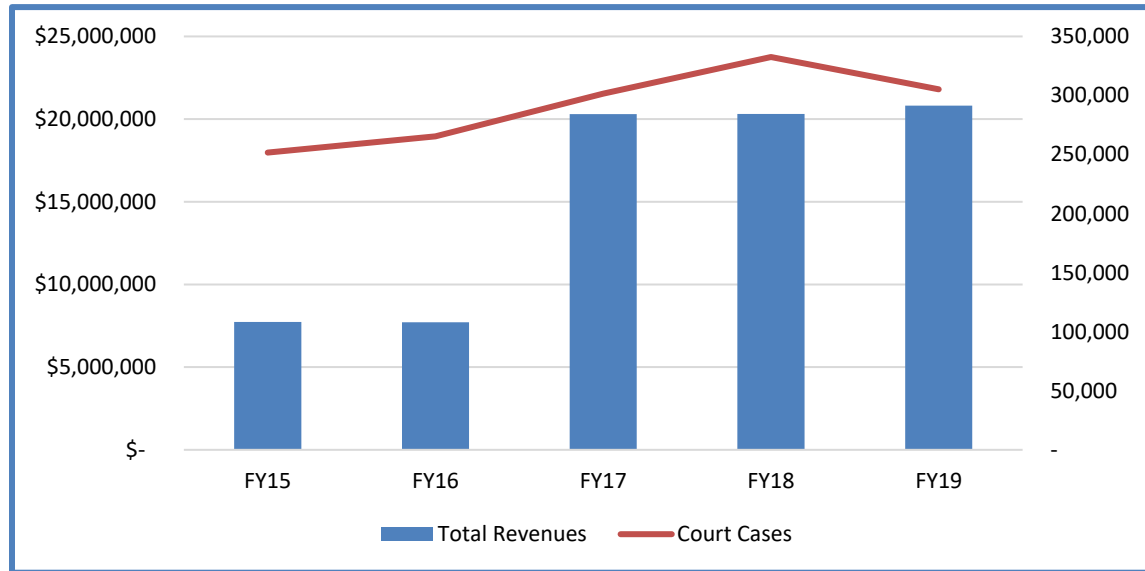


Source: Commonwealth's accounting and reporting system

In reviewing the individual courts, we noted that in the Circuit Court system there is a much closer relationship between revenues and court cases as evidenced in Chart 5, below:

**Revenues – Circuit Courts
(excludes deeds and wills)**

Chart 5

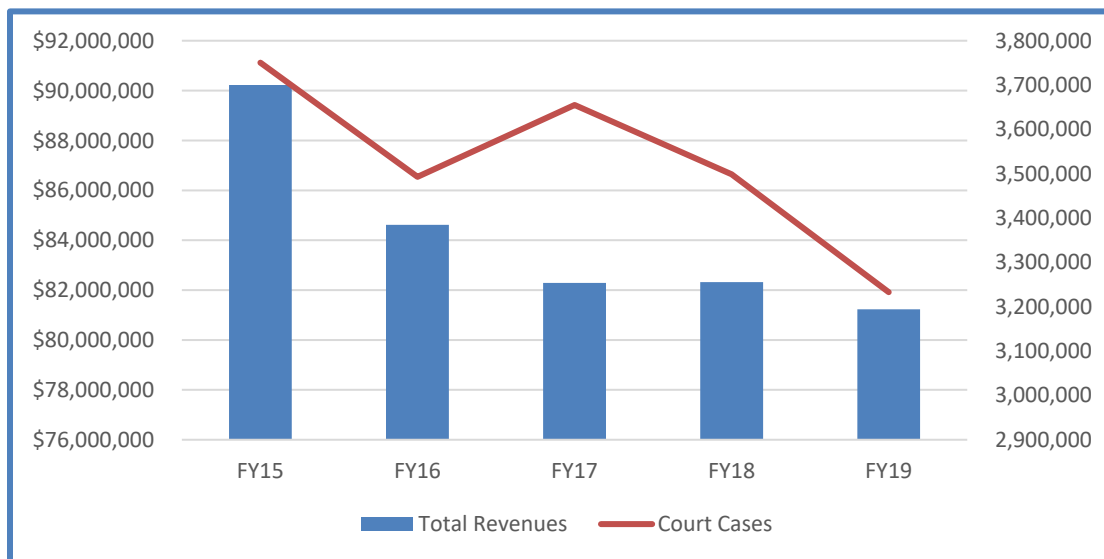


Source: Commonwealth's accounting and reporting system

For the District Court system, there does not appear to be a direct correlation between revenues and number of cases. The district courts hear the greatest number of cases in all the courts system, and these cases range from traffic violations to misdemeanors, to small civil cases which result in extreme changes in revenues depending on the types of cases heard. The relationship is similar to overall cases as evident in Chart 6 below.

Revenues – District Courts

Chart 6



Source: Commonwealth's accounting and reporting system

The Executive Secretary provides a number of administrative services to the Judicial Branch. This includes payroll, human resources, IT services, financial reporting, budgeting, and others. As a result, our scope included the agreements in place to define these services and how responsibilities between agencies in the judicial branch are defined.



Martha S. Mavredes, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

September 10, 2020

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Kenneth R. Plum
Chairman, Joint Legislative Audit
and Review Commission

We have audited the retirement benefits system and information system security control processes of the **Supreme Court of Virginia, Office of the Executive Secretary**, for the fiscal year ended June 30, 2019. We also audited the agreements governing the administrative services the Executive Secretary provides to the Judicial Branch. In addition, we performed analytical procedures over select revenue and expense activity as detailed in the Audit Scope Overview Section. 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 Scope and Objectives

Our audit's primary objectives with regard to the retirement benefits system and information system security control processes, administrative services agreements, and analytical procedures over select revenue and expense activity were to evaluate the accuracy of transactions as recorded in the Commonwealth's accounting and financial reporting system and 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 the prior year reports. We did not review corrective actions for prior audit findings identified as deferred in the [Findings Summary](#) included in the Appendix. We will follow up on these findings in a future audit. See the Findings Summary for a listing of prior year findings and the status of follow-up on management's corrective action.

Audit 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 and regulations.

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 performed analytical procedures, including budgetary and 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 Executive Secretary properly stated, in all material respects, transactions recorded and reported in the Commonwealth's accounting and financial reporting and retirement benefits system, relating to the audit objectives, except as noted in the finding titled "Improve Documentation and Review of Retirement Benefits System Reconciliation" in the section entitled "Status of Prior Year Audit Findings."

We noted certain matters involving internal control and compliance with applicable laws and regulations pertaining to the retirement benefits system, information systems security, and administrative service agreements that require management's attention and corrective action. These matters are described in the section entitled "Status of Prior Year Audit Findings."

The Executive Secretary has taken adequate corrective action with respect to the prior audit finding listed as resolved in the Findings Summary included in the Appendix.

Exit Conference and Report Distribution

We discussed this report with management on October 2, 2020. 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.

Martha S. Mavredes
AUDITOR OF PUBLIC ACCOUNTS

KJS/clj

FINDINGS SUMMARY

Finding	Follow Up Status	Year Last Issued
Continue Improving Database Security	Resolved	2016
Continue to Improve Sensitive Systems Risk Assessment and Contingency Planning Documentation	Repeat*	2016
Maintain Oversight of Third-Party Service Providers	Repeat*	2016
Perform Information Technology Security Audits	Repeat*	2016
Improve Disaster Recovery Controls	Repeat*	2016
Continue Performing a Risk Analysis for Exceptions to the Acceptable Use Policy	Repeat*	2016
Obtain and Retain an Information Security Officer	Repeat*	2016
Improve Documentation and Review of Retirement Benefits System Reconciliations	Repeat*	2018
Establish Memoranda of Understanding with Separate Agencies	Repeat*	2018
Correctly Document, Track, and Report Information Technology Project Costs	Deferred**	2017
Perform a Physical Inventory of Capital Assets	Deferred**	2017
Evaluate the Useful Life of Capital Assets	Deferred**	2017
Improve, Document and Implement a Capital Asset Addition Process	Deferred**	2017
Improve, Document, and Implement a Construction in Progress Reconciliation Process	Deferred**	2017

*Follow-up Status on prior year findings identified as “Repeat” indicates sufficient corrective action on a prior recommendation is not complete; therefore, the prior year finding has been fully or partially repeated.

**Follow-up Status on prior year findings identified as “Deferred” indicates review of management’s corrective action on a prior year finding will be performed in a future audit.

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



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

JUDICIAL INFORMATION TECHNOLOGY
MICHAEL J. RIGGS, SR., DIRECTOR
JUDICIAL PLANNING
CYRIL W. MILLER, JR., DIRECTOR
JUDICIAL SERVICES
PAUL F. DELOSH, DIRECTOR
LEGAL RESEARCH
STEVEN L. DALLE MURA, DIRECTOR
LEGISLATIVE & PUBLIC RELATIONS
KRISTI S. WRIGHT, DIRECTOR
MAGISTRATE SERVICES
JONATHAN E. GREEN, DIRECTOR

November 12, 2020

Ms. Martha S. Mavredes
Auditor of Public Accounts
James Monroe Building
101 North 14th Street
Richmond, Virginia 23219

Dear Ms. Mavredes:

Thank you for providing the Office of the Executive Secretary of the Supreme Court of Virginia an opportunity to review the Management Points 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 processes. The following items were communicated to the Office of the Executive Secretary:

Obtain and Retain an Information Security Officer

Salary constraints continue to hamper the onboarding of a full time Information Security Officer (ISO), however our ability to retain the same contract employee since November 2019 has assisted us in identifying and acting upon the duties and processes of the ISO office. These processes include applying the necessary resources at various levels to ensure the information and systems maintained by OES are secure.

Even without this full-time staff person, we have been able to make great progress building out the overall security program and addressing security issues as they arise, just as a formal ISO would do. Continuing those efforts will address many, if not all, of the deficiencies being noted during this audit.

We fully recognize the need for a full-time ISO and plan to continue the search for one within our salary constraints.

Continue to Improve Sensitive Systems Risk Assessment and Contingency Planning Documentation

We have made significant progress in organizing, updating and maintaining the tasks of the ISO office. Concentration has been in the area of completing the review of the

Ms. Martha S. Mavredes
November 12, 2020
Page 2 of 3

application risk assessments, reviewing business impacts of all applications, identifying sensitive systems (26 of the 29 applications completed) and working on the rollout of the new security awareness program launched in March 2020. Following completion of the risk assessment task and approval of same, we will be able to start on proper contingency planning reviews.

The ISO contract employee has also been instrumental in formatting and organizing an ISO task matrix that will better help the organization identify and maintain consistencies in review, modifications and continued strengthening of the ISO office.

Improve Disaster Recovery Controls

In October 2018, the Office of the Executive Secretary moved all production processing hardware, i.e. mainframe, DASD towers, rack servers, tape units, switches etc. to a secured location at QTS. This QTS site provides collocation services including guaranteed redundancies in electrical, cooling, telco as well as facility security. We have up to date maintenance plans in place for all our equipment, all with 8 hours response time or less. The QTS facility exceeds FISMA High physical security and environmental control environments requirements. QTS personnel have no access to OES data or systems.

We continue to explore cost efficient ways of replicating our production environment needs to establish a viable disaster recovery plan that provides full coverage for any incident encountered at QTS. However, a budget amendment would be needed in order to establish a fully functional hot site.

Maintain Oversight of Third-Party Service Providers

Although not formally documented, the OES contract ISO has started on the process of maintaining oversight for those third-party entities defined as providers. Through verbal communications between the APA and ISO, we were able to provide the necessary information (SOC, HiTrust and Security reports) requested. A more formal process will be put into place to codify the process and procedures in order to perform an annual review of these providers.

Perform Information Security Audits

Independent, third-party audits will have a significant impact on an already stretched budget, however we understand the importance of this review.

It is important to note that all applications, deemed sensitive or not, undergo thorough testing for vulnerabilities using acquired tools and methods meant to expose such risks.

Ms. Martha S. Mavredes
November 12, 2020
Page 3 of 3

In addition, we have deployed multi-layered cyber-security tools to enhance the security of our network, applications and data.

Continue Performing a Risk Analysis for Exceptions to the Acceptable Use Policy

The Acceptable Use Policy scope has been modified to require exceptions granted be in writing by the Executive Secretary. It is recognized that an annual review of those exceptions should be conducted. In the ongoing effort to identify and prioritize the tasks of the Information Security Officer, this will be added to the responsibilities of the ISO.

Establish Memoranda of Understanding with Separate Agencies

The Office of the Executive Secretary recognizes that the development of a formal Memoranda of Understanding with the Virginia Criminal Sentencing Commission and the Judicial Inquiry & Review Commission for administrative and payroll services would be beneficial. It would define the responsibilities of each agency and the services that are being provided.

Improve VNAV Documentation and Review

The Supreme Court of Virginia acknowledges the importance of maintaining documentation of the reconciliations done between our human resources system and the Commonwealth's retirement system. New policies and procedures are being developed and documented to address this finding.

Finally, I would like to express my appreciation to your audit team for their professionalism and willingness to work with my staff to perform this audit in a way that ensured the safety of all personnel during this ongoing pandemic.

With best wishes, I am

Very truly yours,



Karl R. Hade

KRH/mj

**OFFICE OF THE EXECUTIVE SECRETARY
OF THE
SUPREME COURT OF VIRGINIA**

As of June 30, 2019

The Honorable Donald W. Lemons
Chief Justice

Karl R. Hade
Executive Secretary