


OFFICE OF THE EXECUTIVE SECRETARY
OF THE SUPREME COURT OF VIRGINIA
CLERK OF THE SUPREME COURT
CLERK OF THE COURT OF APPEALS
THE JUDICIAL INQUIRY AND REVIEW COMMISSION
VIRGINIA CRIMINAL SENTENCING COMMISSION

REPORT ON AUDIT
FOR THE YEARS ENDED
JUNE 30, 2012 AND JUNE 30, 2013

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

AUDIT SUMMARY

This report includes the Office of the Executive Secretary of the Supreme Court of Virginia, Clerk of the Supreme Court, Clerk of the Court of Appeals, the Judicial Inquiry and Review Commission, and the Virginia Criminal Sentencing Commission (Judicial Agencies). Our audit of these agencies for the fiscal years ended June 30, 2012, and June 30, 2013, found:

- proper recording and reporting of transactions, in all material respects, in the Commonwealth Accounting and Reporting System and the Supreme Court's Integrated Decision Support System;
- internal control matters that require management's attention and corrective action, which are included in the section entitled "Audit Findings and Recommendations;" and
- instances of noncompliance with applicable laws and regulations that are required to be reported under Government Auditing Standards, which are included in the section entitled "Audit Findings and Recommendations."

–TABLE OF CONTENTS–

AUDIT FINDINGS AND RECOMMENDATIONS

Track Internal Software Development Costs – Repeat Finding

The Office of the Executive Secretary of the Supreme Court of Virginia (OES) does not have a method for tracking its internal software development costs. Since 2007 we have recommended the Department of Judicial Information Technology (DJIT) track all time and costs, including internal staffing. DJIT's failure to track internal time has resulted in best guess estimates when assigning internal costs to systems development projects. DJIT has historically viewed the internal development costs as sunk costs and has not seen the value in tracking them by project. In addition, the Fiscal Department has not verified the number given to them from DJIT before including it on the intangibles line item of its financial statements.

The Governmental Accounting Standards Board (GASB) No. 51, Accounting and Financial Reporting for Intangible Assets, establishes the requirements for expensing and capitalizing internal software development costs. These costs are reported to the Department of Accounts for inclusion in the statewide Comprehensive Annual Financial Report (CAFR) and are reported in the Fixed Assets Accounting System (FAACS).

We recommend the OES implement a method to track all internal costs related to software development for proper capitalization and expensing. Although the Fiscal Department has communicated with DJIT the requirements regarding the tracking of internal costs and GASB 51, DJIT still has not implemented a process to track these costs. Therefore, we also recommend that the Fiscal Department verify the intangible assets number provided by DJIT before including it in the annual financial statements.

Distinguish Between Project and Enhancement

The OES does not have defined criteria for the difference between a project and an enhancement or upgrade and; therefore, lacks the appropriate documentation for some projects. The Project Management Body of Knowledge (PMBOK), nationally recognized as a best practice and published by the Project Management Institute, defines a project as a temporary endeavor undertaken to create a unique product, service, or result.

The Virginia Judicial Electronic Filing system (VJEFS) added a new major service in 2013. Based on the PMBOK definition of a project, the creation of a unique service would consider the changes made to VJEFS as a new project. Due to the lack of a definition between enhancement and project, the VJEFS file did not contain the necessary documentation required by OES's policies and procedures for creation of a new project. The risk of not having a project properly documented is that there is no evidence of the plan and the decisions that are made to support the budget, schedule, and requirements. As a result, there is a likelihood the project could go over budget, be behind schedule, or not be what the end user requested.

We recommend that DJIT and the Project Management Office work together to commit in writing to a definition of the difference between a project and an enhancement and add it to their project classification documentation. They should also specify the appropriate category on their current information technology project inventory listing since they maintain upgrades, enhancements, and projects all on a common list.

Improve Database Security – Repeat Finding

The OES continues to inadequately protect sensitive systems by not preventing back end users from accessing and/or editing database and system audit logs.

According to Center for Internet Security benchmarks, an industry best practice, database and system audit logs are to be secured in such a way as to prevent any unauthorized party, including database and system administrators, from modifying or deleting the audit logs generated by database and system activity. In the previous OES audit, we determined, and OES concurred, that the database and system audit logs for the Case Management System (CMS) and Financial Management System (FMS) are not sent to a centralized log server where they are protected from unauthorized modification or deletion. We also determined, and OES concurred, that OES had no process in place to monitor and review the related logs to ensure data integrity, and detect anomalous and suspicious activity. The Commonwealth Security Standard, SEC 501-08, at section IR-1-COV, requires at a minimum that an information security monitoring and logging practice be defined, and include a procedure for aggregating system log information. SEC 501-08 further requires at a minimum, at section AU-3, that logging be implemented on all systems that includes events, users ID associated with the event, and the time of occurrence. During the current audit, we determined that OES has made no progress towards addressing the related control weaknesses over the past two fiscal years.

This internal control weakness continues to present the risk that, if an external party with malicious intent were able to access the system and its sensitive data, they would be able to modify, copy, or delete CMS and FMS information and modify the system and database audit logs to remove any evidence of their activities. It also continues to present the risk that if an internal party with elevated systems access, such as a system or database administrator, were to become disgruntled, they would also be able to cover up any of their activities by modifying the related audit logs. When system and database administrators have the ability to alter audit logs, OES cannot rely upon these logs to track user activity and ensure there are no unauthorized changes to critical data, thus increasing the risk of fraud.

We continue to recommend that OES assess all of its critical systems and database audit logs, and configure them to be automatically exported and stored on a secure external log server where the logs cannot be altered. We also recommend that OES implement a process to review the secure systems and database audit logs for anomalies, either manually or with an automated tool, on a reoccurring basis. This will help mitigate the risk of unauthorized changes being made and help monitor for malicious and anomalous system activity.

Improve Information Security Program – Repeat Finding

OES is still not in compliance with the Commonwealth's information security standards that require agencies to document, approve, and implement policies and procedures which establish how sensitive data should be consistently safeguarded. In the previous OES audit, we determined, and OES concurred, that OES had not implemented any of the following information security policies and procedures:

- Acceptable Use of Technology Resources
- Account and Access Control Policy
- Cryptographic Key Management Policy
- Data Breach Notification Policy
- Data Encryption Policy
- Data Storage Media Protection Policy
- Email Communication Policy
- Facilities Security Policy
- Information Security Log Management Policy
- Information Security Policy
- Information Technology Systems Hardening Policy
- Password Policy
- Security Awareness Training Policy
- Systems Interoperability Policy

We further determined, and OES concurred, that OES has no documented policies, procedures, or processes in its security program for the following areas:

- Change Management over Infrastructure and Applications
- Rule-Set Reviews
- Disaster Recovery
- Remote Access
- Technical Employee Security Training
- IT System and Data Backup and Restoration Policy
- Records Retention Policy
- Malicious Code and Virus Protection Policy

In the current year audit, we determined that OES has not made significant progress in augmenting the OES Security Program to improve its security posture since the previous audit. We determined that instead, OES Security has been focusing on building a systems interface to facilitate less manual processes for Security Awareness and Training for their internal network end user population.

Identifying, documenting, and implementing policies and procedures continues to be the primary method for OES's management team to develop an information security program and to

communicate their expectations to employees on how sensitive data should be protected. Without documenting these processes, and communicating and training employees on them, OES cannot efficiently, effectively, or consistently implement security controls that meet industry best practices.

An appropriately documented information security program will reduce the risk of misconfigured infrastructure devices and applications that may inadvertently allow malicious internet traffic to penetrate the Supreme Court's network. In addition to allowing for improved network management practices, documenting the procedures will enable a much smoother transition of personnel when turnover occurs at OES.

We continue to recommend that OES develop and implement policies and procedures in these areas for its information security program. We also recommend that the OES's information security officer regularly review the policies and procedures to ensure that they follow current industry best practices and that staff are properly trained in implementing those requirements.

Realign Information Security Officer with Industry Best Practices – Repeat Finding

The Information Security Officer (ISO) at OES still does not have information security oversight and authority to all departments or information technology projects that produce and manage confidential and mission critical data within the organization.

In the previous OES audit, we determined that the ISO has no oversight or authority over the other OES departments including the Assistant Executive Secretary and Counsel, the Court Improvement Program, Educational Services, Fiscal Services, the Historical Commission, Human Resources, Judicial Planning, Judicial Services, Legal Research, and Legislative and Public Relations. We also determined that the ISO only has limited oversight over the Judicial Information Technology Department. We further determined that these departments manage and create confidential and mission critical data and intellectual property.

In the current OES audit, we determined that no significant changes have occurred and the OES ISO continues to have limited oversight and security governance across the enterprise. We also determined that because of this lack of oversight by the ISO, no consistent process exists for the removal of all system access across the organization when an employee terminates. One in seven employees (14 percent) tested did not have CARS systems access terminated on a timely basis. We determined that, due to the lack of security governance, OES has not implemented its IT Systems Access Security Policy for all IT Systems. One user out of 11 tested (nine percent) had the ability to both key and release batches in the Integrated Decision Support System (IDSS), while not requiring either role for their job function. This violates the concept of least privilege as required by the OES IT Systems Access Security Policy and the Commonwealth Security Standard, SEC 501-08.

These results validate the fact that without appropriate alignment of the ISO role and information security governance in the organization, the OES will continue to operate at an increased risk in the following areas.

- Confidential and mission critical data will not be appropriately protected.
- Segregation of duties will not be maintained within systems across departments.
- Least privilege access to systems will not be applied on a departmental basis.
- Security will not be a building block in all ongoing IT projects.

We recommend that OES realign the ISO position in the organization to govern, implement, and enforce its information security policy for all of the departments under OES and be required to be formally involved in all IT projects in the future throughout the Court System.

Continue to Improve Sensitive Systems Risk Assessment and Contingency Planning Documentation – Repeat Finding

OES continues to inappropriately consider business and systems security risks when its network environment and sensitive systems go through major upgrades and material changes, or at least once every three years. According to the Commonwealth of Virginia (COV) Information Security Standard, SEC 501-08, agencies are required to "conduct periodic review and revision of the agency Business Impact Analysis, as needed, but at least once every three years" and "conduct and document a Risk Assessment of the IT system as needed, but not less than once every three years."

During the previous audit, we found that OES had not performed a review of the agency Business Impact Analysis or a Risk Assessment for the Case Management System (CMS) in the last three years. OES' systems environment has dynamically changed since the last Business Impact Analysis in November of 2007. Additionally CMS has undergone significant system upgrades since OES performed the last Risk Assessment in March of 2009. During the current audit, we determined that OES has made no significant progress in updating either the Business Impact Analysis or the CMS Risk Assessment in the past two fiscal years.

As the OES Business Impact Analysis and CMS Risk Assessment no longer reflect the related business or system risks, OES continues not to employ the appropriate measures to identify or consider the vulnerabilities and risks in its business and systems environment. Risk assessments aid in identification, analysis, and mitigation of risks that could compromise OES' IT systems. Using these risk assessments, OES can prioritize security, contingency, and disaster recovery efforts in high risk areas, and ensure the availability of critical data and protection of sensitive data.

We recommend that OES continue to improve its Information Systems Security Program by complying with the requirements of SEC 501-08 by updating its Business Impact Analysis when the business systems environment changes and completing risk assessments for all sensitive systems when upgrades are performed, or at least once every three years. In addition, we recommend that OES utilize the results of this process to appropriately update its contingency planning, incident response, and disaster recovery documentation in order to assess and mitigate identified threats and vulnerabilities in the OES environment.

AGENCY HIGHLIGHTS

Office of the Executive Secretary of the Supreme Court

Section 17.1-314 of the Code of Virginia establishes the Office of the Executive Secretary of the Supreme Court to serve as the court administrator for the Commonwealth. The Office of the Executive Secretary maintains the Court Automated Information System, which accumulates financial and case information for the courts. In addition, the Office of the Executive Secretary provides statewide fiscal and human resource administration for the following courts and agencies:

- Circuit Courts (Judges only)
- Clerk of the Supreme Court
- Combined District Courts
- Court of Appeals
- General District Courts
- Judicial Inquiry and Review Commission
- Juvenile and Domestic Relations District Courts
- Magistrates
- Virginia Criminal Sentencing Commission

Supreme Court Financial Information

Supreme Court appropriations and expenses include the cost of the Office of the Executive Secretary, the Clerk of the Supreme Court, and judicial policymaking bodies. The judicial policymaking bodies include the Judicial Council, Committee on District Courts, Judicial Conference of Virginia, and the Judicial Conference of Virginia for District Courts. The following table summarizes the actual expenses for the Supreme Court of Virginia for fiscal years 2012 and 2013.

Analysis of Actual Expenses for Fiscal Years 2012 and 2013

	2012	2013
Personal Services	$ 18,143,688	$ 19,305,763
Contractual Services	12,267,052	11,778,242
Supplies and Materials	159,917	154,919
Transfer Payments	2,856,447	2,732,444
Plant and Improvements	2,250	1,850
Continuous Charges	2,133,512	2,407,850
Equipment	555,402	1,000,852
Total	$ 36,118,268	$ 37,381,920

Source: Commonwealth Accounting and Reporting System

Expenses consist mostly of payroll and contractual services. The majority of contractual service expenses are information technology costs related to the Court Technology Fund.

Court of Appeals

The Court of Appeals of Virginia provides appellate review of final decisions of the Circuit Courts in domestic relations matters, appeals from decisions of an administrative agency, traffic infractions, and criminal cases, except when there is a sentence of death. It also hears appeals of final decisions of the Virginia Workers' Compensation Commission. There are petitions for appeal for criminal, traffic, concealed weapons permit, and certain preliminary rulings in felony cases. All other appeals to the Court of Appeals are a matter of right. Petitions for appeal that occur for other Circuit Court civil decisions go directly to the Supreme Court of Virginia.

The decisions of the Court of Appeals are final in traffic infraction and misdemeanor cases where there is no incarceration, domestic relations matters, and cases originating before administrative agencies or the Virginia Workers' Compensation Commission. Except in those cases where the decision of the Court of Appeals is final, any party aggrieved by a decision of the Court of Appeals may petition the Supreme Court for an appeal.

The Court of Appeals consists of 11 judges. The court sits in panels of at least three judges, and the panel membership rotates. The court sits at such locations as the chief judge designates, to provide convenient access to the various geographic areas of the Commonwealth.

The following table summarizes the actual expenses for the Court of Appeals for fiscal years 2012 and 2013. The majority of expenses in both fiscal years are related to personal services.

Analysis of Actual Expenses for Fiscal Years 2012 and 2013

	2012	2013
Personal Services	$7,873,796	$8,119,252
Contractual Services	276,088	237,661
Supplies and Materials	23,063	4,346
Transfer Payments	73	14,276
Continuous Charges	526,779	430,670
Equipment	29,308	49,322
Total	$8,729,107	$8,855,527

Source: Commonwealth Accounting and Reporting System

Judicial Inquiry and Review Commission

The Judicial Inquiry and Review Commission investigates allegations of judicial misconduct or the serious mental or physical disability of a judge. The Commission has jurisdiction to investigate the justices of the Supreme Court and all judges of the Commonwealth, as well as members of the State Corporation Commission, the Virginia Workers' Compensation Commission, special justices, substitute judges, and retired judges who have been recalled to service. The Commission may file a formal complaint with the Supreme Court against judges for violations of any canon of judicial ethics, misconduct in office, or failure to perform judicial duties.

The Commission has seven members elected by the General Assembly and members serve four-year terms. Membership includes one Circuit Court judge, one General District Court judge, one Juvenile and Domestic Relations District Court judge, two lawyers, and two members of the public who are not attorneys.

The following table summarizes the actual expenses for the Judicial Inquiry and Review Commission for fiscal years 2012 and 2013. The majority of expenses in both fiscal years are related to personal services.

Analysis of Actual Expenses for Fiscal Years 2012 and 2013

	2012	2013
Personal Services	$ 442,450	$ 436,955
Contractual Services	26,749	32,194
Supplies and Materials	6,793	3,479
Continuous Charges	52,046	52,786
Equipment	2,388	8,061
Total	$ 530,426	$ 533,475

Source: Commonwealth Accounting and Reporting System

Virginia Criminal Sentencing Commission

The Virginia Criminal Sentencing Commission develops sentencing guidelines to ensure consistent punishments for offenses in all felony cases. It is currently composed of 17 members including seven judges, five legislators, four Governor Appointees, and the Attorney General.

The following table summarizes the actual expenses for the Virginia Criminal Sentencing Commission for fiscal years 2012 and 2013. The majority of expenses in both fiscal years are related to personal services.

Analysis of Actual Expenses for Fiscal Years 2012 and 2013

	2012	2013
Personal Services	$ 749,377	$ 690,665
Contractual Services	71,268	87,864
Supplies and Materials	43,933	7,538
Transfer Payments	15,315	2,712
Continuous Charges	58,877	60,922
Equipment	12,902	10,113
Total	$ 951,672	$ 859,814

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

July 29, 2014

The Honorable Terence R. McAuliffe
Governor of Virginia

The Honorable John C. Watkins
Chairman, Joint Legislative Audit
and Review Commission

We have audited the financial records and operations of the **Office of the Executive Secretary of the Supreme Court of Virginia, Clerk of the Supreme Court, Clerk of the Court of Appeals, the Judicial Inquiry and Review Commission, and the Virginia Criminal Sentencing Commission (Judicial Agencies)** for the years ended June 30, 2012, and June 30, 2013. 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 Accounting and Reporting System and the Supreme Court's Integrated Decision Support System, review the adequacy of the Judicial Agencies' internal controls, test compliance with applicable laws, regulations, contracts, and grant agreements and review corrective actions of audit findings from prior year reports.

Audit Scope and Methodology

The Judicial Agencies' management has responsibility for establishing and maintaining internal control and complying with applicable laws and regulations. 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.

Payroll, travel and other expenses	Systems security
Cash receipts	Systems access
Criminal fund expenses	Systems development
Involuntary Mental Commitment fund expenses	Billing to Local Courts
IT Sole Source Procurement	Federal Grants

We performed audit tests to determine whether the Judicial Agencies' 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 Judicial Agencies' operations. We tested transactions and performed analytical procedures, including budgetary and trend analyses.

Conclusions

We found that the Judicial Agencies properly stated, in all material respects, the amounts recorded and reported in the Commonwealth Accounting and Reporting System and the Supreme Court's Integrated Decision Support System. The Judicial Agencies record their financial transactions on the cash basis of accounting, which is a comprehensive basis of accounting other than accounting principles generally accepted in the United States of America. The financial information presented in this report came directly from the Commonwealth Accounting and Reporting System.

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

The Judicial Agencies have taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this letter.

Exit Conference and Report Distribution

We discussed this report with management on September 15, 2014. Management's response to the findings identified in our audit is included in the section titled "Agency Response." Our comments related to management's response are included in the section titled "APA Comments on Management's 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.

AUDITOR OF PUBLIC ACCOUNTS

LJH/alh

EXECUTIVE SECRETARY
KARL R. HADE

ASSISTANT EXECUTIVE SECRETARY &
LEGAL COUNSEL
EDWARD M. MACON

COURT IMPROVEMENT PROGRAM
LELIA BAUM HOPPER, DIRECTOR

EDUCATIONAL SERVICES
CAROLINE E. KIRKPATRICK, DIRECTOR

FISCAL SERVICES
JOHN B. RICKMAN, DIRECTOR

SUPREME COURT OF VIRGINIA

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

HUMAN RESOURCES
RENÉE FLEMING MILLS, DIRECTOR

JUDICIAL INFORMATION TECHNOLOGY
ROBERT L. SMITH, 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

September 22, 2014

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

Dear Ms. Mavredes:

Thank you for providing us the opportunity to review the draft audit report for the Supreme Court of Virginia for the period July 1, 2011, through June 30, 2013. As we discussed in our meeting on August 15, 2014, I wanted to share with you additional information regarding the recommendations contained in this audit report.

Recommendation – Track Internal Software Development Costs

Project budgets are determined and tracked by the DJIT Director. Projects and budgets are submitted to the Executive Secretary for approval and prioritization. Project costs (including hardware, software, and consultants) are reviewed each month as part of a budget review meeting with the Executive Secretary. Project priorities are also discussed in these meetings and all resources, including internal resources, are reviewed and reallocated as needed to support any change in priorities.

Going forward, DJIT will work with the Fiscal department to develop a methodology to add in internal resource costs to comply with the GASB No. 51 requirements.

Recommendation – Define Project versus Enhancement

Since our last audit, we have made substantial progress in enhancing our project management processes and oversight. This progress includes selecting a full-time PMO Manager, implementing a new project approval process, developing document templates to use throughout the project lifecycle, and implementing a structured project status reporting process. As we continue growing our project management structure, we will incorporate guidelines on identifying projects versus enhancements.

Upon closer review, we believe the VJEFS work should have been classified as an enhancement, not a new project. However; the oversight that our processes provided helped to ensure that this enhancement was implemented on time and under budget.

Recommendation – Improve Database Security

Sensitive databases are protected from access by external parties in a variety of manners. Server security, database security, network security and network monitoring all play a role in protecting these databases from external parties. These safeguards have been tested through ethical hacking engagements and internal reviews of our security posture.

Internally, access to sensitive databases is determined by the principle of least privilege and very few individuals have such access.

While the threat to these databases is minimal, we do agree that compliance with SEC 501-07 is critical to fully protect the sensitive data under our control. We also agree that our current database and system audit logs need to be secured in such a manner to prevent these logs from being modified or deleted.

We recognize that our current logging solution does not provide sufficient capacity to add additional logging functions. Additionally, our current solution does not provide a mechanism for automated log reviews. Procuring a new logging solution has been on hold due to the significant budget reductions over the past two years.

This fiscal year, we will review new logging solutions and make a recommendation for purchase by June 30, 2015.

Recommendation – Improve Information Security Program

In May of 2012, the following policies were approved for implementation:

- Acceptable Use of Technology Resources
- Account and Access Control Policy
- Cryptographic Key Management Policy
- Data Breach Notification Policy
- Data Encryption Policy
- Data Storage Media Protection Policy
- Email Communication Policy
- Facilities Security Policy
- Information Security Log Management Policy
- Information Security Policy
- Information Technology Systems Hardening Policy
- Password Policy
- Security Awareness Training Policy
- Systems Interoperability Policy

Since that time, the OES has worked to implement these policies throughout Virginia's

Judicial Branch of government. This work will continue until all approved policies are fully implemented. Our Information Security officer (ISO) is reviewing various methods to enforce these policies and a recommendation will be forthcoming.

In September of this year, our ISO began performing a gap analysis between our information security program and the State standard, SEC-501. The results of this gap analysis will be incorporated into our ongoing information security program updates.

Since the previous audit, significant progress has been made in the OES Security Program. In 2012, an information security briefing was included in new magistrate and district court clerk training programs. In 2013, we contracted with a company to refresh our system risk assessments, business impact analysis, continuity of operations plans, and disaster recovery plans. This engagement is schedule to be completed in October of 2014. In 2014, we initiated a project to automate the management of our security awareness program so it can be deployed statewide. This project will be completed in the first quarter of 2015.

Recommendation – Realign Information Security Officer with Industry Best Practices

The Information Security Officer does have information security oversight and authority across Virginia's Judicial Branch of government and steps have been taken to enforce that position.

In 2012, the ISO began providing security briefings to incoming magistrates and district court clerks. Briefings are also offered at Virginia's Judicial Conferences for all of Virginia's judges.

In 2013, an information security section was added to new project initiation and the ISO has the authority to stop any IT project if significant security flaws are identified. The ISO also has the authority to go directly to the Executive Secretary and Chief Justice with any security issues.

The ISO has been involved in a number of initiatives to strengthen the Judicial Branch information security posture. These initiatives have spanned across OES departments as well as other Judicial Branch agencies.

We will continue to increase awareness of the ISO's role as well as awareness of information security overall.

Recommendation – Improve Sensitive Systems Risk Assessment and Contingency Planning and Documentation

Over the last 3 years, the ISO has performed multiple risk assessments on various IT systems. In 2012, a project to update existing system risk assessments, business impact analysis, continuity of operations plans and disaster recovery plans was approved. However; budget shortfalls pushed this project to fiscal year 2014. In 2013, the project began and is slated for completion in October of 2014.

This project includes an in depth review of existing documentation, interviews with key stakeholders representing all areas of Virginia's Judicial Branch of government, visits to diverse courts around the Commonwealth, and verification of compliance with SEC-501. Once completed, these documents will be shared, in a secure manner, with the APA. These documents will also help guide the direction of the expansion of our information security program.

With best wishes, I am

Very truly yours,

Karl R. Hade

cc: John B. Rickman
Robert L. Smith

APA's COMMENTS ON MANAGEMENT'S RESPONSE

The Office of the Executive Secretary of the Supreme Court of Virginia's (OES) response to the "Improve Database Security" management recommendation stated that server, database, and network security controls "have been tested through ethical hacking engagements." The last OES ethical hacking engagement, or penetration test, occurred in 2011. Additionally, the 2011 penetration test was of limited scope and did not focus on database management system security controls within the IT environment. Due to the rapidly changing pace of technology and continued increase in external threats, as well as the limited scope external testing performed; it is our opinion that this external engagement has not been performed on a timely or adequate basis to reasonably or appropriately mitigate the risk that we have identified.

The OES response to the "Improve Information Security Program" recommendation stated that "OES has worked to implement these policies throughout Virginia's Judicial Branch of government. This work will continue until all approved policies are fully implemented." OES policies such as the Acceptable Use of Technology Resources Policy and Email Communications Policy explicitly do not include the group of individuals that have the greatest access to the Supreme Court of Virginia's most sensitive data. Justices, Judges, Circuit Court Clerks, the Executive Secretary, OES Directors, the Clerk, Chief Staff Attorney, the Law Librarian of the Supreme Court of Virginia, the Clerk and Chief Staff Attorney of the Court of Appeals are all not bound by either policy and have access to inherently confidential data.

Additionally, the OES Information Security Awareness and Training Policy requires that all users complete the related training before being given access to any sensitive IT system. The policy also requires that users take the related training once annually or more often as needed. During our review we found that OES has more than 5,300 supported end users. In testing the implementation of the OES Information Security Awareness and Training Policy, we identified that of the 5,300 end users, only 283 had actually taken the required training, which is approximately 5.3 percent. OES cannot implement its Information Security Program throughout the Judicial Branch of government until all end users are held accountable to the policy set.

AGENCY OFFICIALS

OFFICE OF THE EXECUTIVE SECRETARY OF THE SUPREME COURT OF VIRGINIA

The Honorable Cynthia D. Kinser, Chief Justice

Karl R. Hade, Executive Secretary

CLERK OF THE SUPREME COURT

Patricia Harrington, Clerk

COURT OF APPEALS OF VIRGINIA

The Honorable Walter S. Felton, Jr., Chief Judge

Cynthia McCoy, Clerk

JUDICIAL INQUIRY AND REVIEW COMMISSION

Katherine B. Burnett, Counsel

VIRGINIA CRIMINAL SENTENCING COMMISSION

Meredith Farrar-Owens, Director