JUDICIAL BRANCH

AUDIT OF
INFORMATION SYSTEMS SECURITY
JUNE 30, 2016

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

AUDIT SUMMARY

Our audit of Information Systems Security of the Judicial Branch, which the Office of the Executive Secretary (Executive Secretary) of the Supreme Court of Virginia provides, for fiscal year 2016, found:

- matters involving internal control and its operation necessary to bring to management's attention;

- instances of noncompliance with the Commonwealth's Information Security Standard, SEC 501-09 (Security Standard) that are required to be reported;

- inadequate corrective action with respect to the following 2013 audit findings:
  - Improve Database Security
  - Continue to Improve Sensitive Systems Risk Assessment and Contingency Planning Documentation; and

- adequate corrective action with respect to the following 2013 audit findings:
  - Improve Information Security Program
  - Realign Information Security Officer with Industry Best Practices.

The following entities of the Judicial Branch receive information system security services from the Executive Secretary, specifically from its department of Judicial Information Technology (Judicial Technology) and, as a result, they should consider the results of this audit:

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

-TABLE OF CONTENTS-

AUDIT FINDINGS AND RECOMMENDATIONS

Obtain and Retain an Information Security Officer

Type: Internal Control and Compliance
Repeat: No

The Executive Secretary does not have an Information Security Officer (ISO) to improve and maintain its information security program. The lack of an ISO led to the identification of other weaknesses, which we discussed in detail in separate recommendations communicated to the Executive Secretary as follows:

- Improve Disaster Recovery Controls
- Continue to Improve Sensitive Systems Risk Assessment and Contingency Planning Documentation
- Continue Improving Database Security
- Maintain Oversight of Third-Party Service Providers
- Perform Information Technology Security Audits
- Perform a Risk Analysis for Exceptions to the Acceptable Use Policy

The 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.

What is an ISO?

The ISO is an individual appointed by the head of an agency to assume responsibility over the agency's information security program. The information security program is a collection of security processes, standards, rules, and procedures that represent the implementation of the security policy. The ISO strives to maintain a balance between supporting the business functions and creating an appropriate control environment when designing the information security program.

Without an ISO, the Executive Secretary cannot effectively improve its security posture and resolve the weaknesses discussed in separate recommendations. This puts the Executive Secretary at risk of not protecting the confidentiality, integrity, and availability of sensitive Commonwealth information.

Our last audit recommended that the Executive Secretary realign its ISO position to report to the Agency Head instead of the Chief Information Officer. Since that audit, the Executive Secretary has organizationally realigned the ISO role. However, since then, the Executive Secretary has had three different ISOs, two of whom stayed with the Executive Secretary for ten months or less. Furthermore, the ISO position has been vacant since June of 2016. The Executive Secretary has not placed a job posting to fill the vacant position since the fall of 2016.

The Executive Secretary should obtain and retain a qualified ISO to improve and maintain the information security program, including the resolution of the above-mentioned weaknesses. This should strengthen the Executive Secretary's information security posture and reduce the risk of possible compromise of mission critical or confidential data.

Improve Disaster Recovery Controls

Type: Internal Control and Compliance
Repeat: No

The Executive Secretary does not have certain critical disaster recovery controls. The details of these control weaknesses have been communicated to management in a separate document marked Freedom of Information Act (FOIA) Exempt under §2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

What are disaster recovery controls?

Disaster recovery controls are the plans and preparation put in place by the agency to restore their mission critical business functions and supporting information technology systems in the event that their primary resources are unavailable.

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.

The Executive Secretary should obtain the necessary resources to improve its disaster recovery controls described in the FOIA Exempt 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.

Continue to Improve Sensitive Systems Risk Assessment and Contingency Planning Documentation

Type: Internal Control and Compliance
Repeat: Yes

The Executive Secretary continues to not consider business and system security risks appropriately when its IT environment undergoes major upgrades and material changes.

The prior audit performed for fiscal year 2013 identified that the Executive Secretary had not reviewed and revised the Business Impact Analysis (BIA) and Risk Assessment (RA) at least once every three years or when changes occur within the environment. In 2012, the Executive Secretary hired an external firm to update risk management and contingency planning documentation, including the BIA, RAs, Continuity of Operations Plan (COOP), and Disaster Recovery Plan (DRP). The Executive Secretary accepted the updated documents in 2013. However, our current audit identified that the Executive Secretary does not fulfill seven IT risk management and contingency requirements as set forth in Security Standard. The details of these control weaknesses have been communicated to management in a separate document marked FOIA Exempt 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 ISO is responsible for developing and managing the Executive Secretary's information security program, including the Executive Secretary's risk management and contingency planning documentation, to meet or exceed Commonwealth IT security policies and procedures. The long-term vacancy of an effective ISO contributes significantly to the seven control weaknesses.

What are Risk Management and Contingency Planning documents?

The Risk Management and Contingency Planning documentation includes the BIA, RA, COOP, and DRP. Together, they allow the agency to identify risks, vulnerabilities, and mitigating controls for its information technology environment and business critical functions. Together, they aid the agency in developing its plans to get information systems up and running in the event of an unexpected outage.

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 separate FOIA Exempt communication. Additionally, the Executive Secretary should expedite its recruitment efforts to hire and retain an effective ISO to improve its information security posture to meet or exceed Commonwealth IT security policies and procedures.

Continue Improving Database Security

Type: Internal Control and Compliance
Repeat: Yes
Prior Title: Improve Database Security

The Executive Secretary continues its progress to improve database security. During the prior audit for fiscal year 2013, we recommended that the Executive Secretary implement a security control for two sensitive systems. Since the prior audit, the Executive Secretary has installed a centralized system as a mitigating control to resolve the identified weakness; however, the Executive Secretary is still in progress of developing a formal process for this control. The details of the control weakness have been communicated to management in a separate document marked FOIA Exempt under §2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

What is the ISO's role in database security?

The ISO is responsible for implementing and maintaining the appropriate balance of preventative, detective, and corrective controls for agency IT systems, including databases, commensurate with data sensitivity, risk and criticality.

The ISO is responsible for developing and managing the Executive Secretary's information security program to meet or exceed Commonwealth IT Security policies and procedures, which includes implementing and maintaining the appropriate balance of preventative, detective, and corrective controls for IT systems. The long-term absence of an effective ISO contributed to the Executive Secretary not meeting its goal of resolving the issue in the 60 months since we first reported the issue to the Executive Secretary.

The Executive Secretary should continue its progress towards implementing a formal process for the weakness communicated in the FOIA Exempt document. Additionally, the Executive Secretary should dedicate the necessary resources to recruit for and retain an effective ISO to improve its information security posture to meet or exceed Commonwealth IT security policies and procedures.

Maintain Oversight of Third-Party Service Providers

Type: Internal Control and Compliance
Repeat: No

The Executive Secretary does not have an established 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 that 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 Standard), Section SA-1, requires the Executive Secretary to develop, document, and implement appropriate system and services acquisition policies and procedures. Also, Section SA-9-COV-3 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 provider's internal controls, the Executive Secretary cannot consistently validate that those providers have effective security controls to protect its mission critical and confidential data.

The ISO is responsible for developing and managing the Executive Secretary's information security program to meet or exceed Commonwealth IT security policies and procedures, including the development of a formal framework to maintain oversight of Providers. The long-term absence of an effective ISO allowed for the absence of certain security measures to occur.

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. The evaluation will allow the Executive Secretary to determine whether providers' security controls comply with the requirements described in the security Standard and documented contract agreement.

Why is the ISO responsible for the controls of Providers?

In instances where agencies procure third parties to perform a service, the outsourced service must still maintain compliance with applicable standards, including the Security Standard. The agency head is accountable for this oversight; however, he or she delegates this responsibility for information security controls to the ISO as part of the information security program.

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. Finally, the Executive Secretary should recruit a qualified ISO to improve and maintain its information security posture to meet or exceed the Security Standard.

Perform Information Technology Security Audits

Type: Internal Control
Repeat: No

The Executive Secretary does not perform information technology security audits over its IT systems classified as sensitive on a periodic basis. Currently, the Executive Secretary has 31 sensitive systems identified in its risk management and contingency planning documentation; and while our office audits certain control areas, not all of the control areas for all systems have received the necessary independent security audit. The performance of IT security audits ensure that sensitive systems are configured and maintained in compliance with the Executive Secretary's policies and procedures, the Security Standard, and industry best practices.

By not having periodic IT security audits performed on sensitive systems , the Executive Secretary is increasing the risk for system vulnerabilities and threats within the systems' configuration settings and system management processes to go undetected and not effectively remediated. This puts the Executive Secretary at risk for malicious users to exploit those vulnerabilities to possibly compromise sensitive information and potentially cause systems to become unavailable.

The ISO is responsible for developing and managing the Executive Secretary's information security program to meet or exceed Commonwealth IT security policies and procedures, including implementing and maintaining appropriate preventative, detective, and corrective controls. The long-term absence of an effective ISO allowed this oversight to occur.

The Executive Secretary should develop and maintain an IT security audit plan to schedule all sensitive systems to receive an IT security audit on a periodic basis. Next, as the Executive Secretary does not have an Internal Audit function, the Executive Secretary should have an external audit firm perform IT security audits over its sensitive systems in accordance to the audit plan and resolve any vulnerabilities identified as a result of the audits. Finally, the Executive Secretary should recruit a qualified ISO to improve its information security posture to meet or exceed the Security Standard and industry best practices.

Perform a Risk Analysis for Exceptions to the Acceptable Use Policy

Type: Internal Control and Compliance

Repeat: No

The Executive Secretary does not perform a risk analysis for exceptions made to certain information security policies and controls. The Executive Secretary implemented an Acceptable Use Policy that prohibits the use of computer or network resource to access pornography, gaming sites or audio/video entertainment for non-business purposes. However, the Executive Secretary excludes executive level personnel and magistrates from the Acceptable Use Policy, such as Justices of the Supreme Court of Virginia, Judges of the Court of Appeals of Virginia, circuit court clerks, and the Executive Secretary directors and does not have a documented risk analysis of this exception.

What is an Acceptable Use Policy?

An Acceptable Use Policy communicates the constraints and practices that users must agree to when using the Commonwealth's network and internet. Users sign the policy to acknowledge their expectations so that management can hold them accountable for deviations.

The Security Standard, Section RA-3, requires the Executive Secretary to conduct a risk assessment that evaluates 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.

By not performing and documenting a risk analysis, the Executive Secretary cannot ensure that any compensating controls adequately mitigate the risks presented by allowing exceptions to the Acceptable Use Policy. Additionally, the Executive Secretary cannot ensure continuity in its information security program because it does not document management's decisions to carry forward through turnover and changes in the IT environment.

The absence of a risk analysis occurred due to the lack of an ISO and other competing priorities to improve its information security program. The ISO is responsible for developing and managing the Executive Secretary's information security program to meet or exceed the Security Standard, which includes identifying and evaluating risks within the IT environment to recommend the implementation of mitigating security controls.

The Executive Secretary should perform a risk analysis for providing certain employees with an exception to the acceptable use policy. The analysis should include the 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.

AUDIT SCOPE OVERVIEW

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

As part of the Executive Secretary, the department of Judicial Information Technology (Judicial Technology) serves as the information technology service provider to the judicial branch. In addition to providing information technology services, Judicial Technology implements the control environment for information technology and security for all judicial agencies.

Information security controls include any protective action, device, procedure, technique, or other measure that reduces exposure of the agency's information. They are critical to protect data from malicious compromise and exploitation as well as safeguard its integrity and confidentiality. Information security controls can be divided into families based on the type of control. We tested the following control families as part of our audit:

- Access Controls
- Awareness and Training
- Audit and Accountability
- Contingency Planning
- Physical and Environmental Protection
- Risk Assessment

Our scope focused on information technology security controls in these areas because of multiple management recommendations in the prior audit. This report is located at www.apa.virginia.gov under the title Virginia's Judicial System for the years ended June 30, 2012 and June 30, 2013.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

August 24, 2017

The Honorable Donald W. Lemons
Chief Justice of the Supreme Court of Virginia

The Honorable Robert D. Orrock, Sr.
Chairman, Joint Legislative Audit
and Review Commission

We have audited **Information System Security provided to the Judicial Branch by the Office of the Executive Secretary (Executive Secretary) of the Supreme Court of Virginia** for the year ended June 30, 2016. 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 objective was to evaluate information system security internal controls of the Executive Secretary, including testing for compliance with applicable laws and regulations and following up on prior report audit findings titled "Improve Database Security," "Improve Information Security Program," "Realign Information Security Officer with Industry Best Practices," and "Continue to Improve Sensitive Systems Risk Assessment and Contingency Planning Documentation." We will follow up on the remaining prior report audit findings titled "Track Internal Software Development Costs" and "Distinguish between Project and Enhancements" in subsequent audits.

Audit Scope and Methodology

Management of the Executive Secretary has responsibility for establishing and maintaining information system security internal controls and complying with applicable laws and regulations for the judicial branch. Information system security internal controls are a process designed to provide reasonable, but not absolute, assurance regarding the availability, integrity, and confidentiality of data and information systems.

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 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, placed in operation, and followed. Our audit also included tests of compliance with provisions of applicable laws and regulations as they pertain to our audit objectives.

Our audit procedures included inquiries of appropriate personnel, inspection of documents, records, and observation of the Executive Secretary's operations.

Conclusions

We noted certain matters pertaining to information system security involving internal control and its operation and compliance with applicable laws and regulations that require management's attention and corrective action. These matters are described in the section entitled "Audit Findings and Recommendations."

The agency has taken adequate corrective action with respect to audit findings included in the prior report that are listed under the "Audit Objectives" section of this letter and not repeated in this report.

Exit Conference and Report Distribution

We discussed this report with management on August 24, 2017. 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 of the Supreme Court of Virginia and General Assembly, management, and the citizens of the Commonwealth of Virginia and is a public record.

AUDITOR OF PUBLIC ACCOUNTS

GDS/clj

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
JOHN B. RICKMAN, 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
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

MAGISTRATE SERVICES
MASON L. BYRD, DIRECTOR

August 31, 2017

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, 2015, through June 30, 2016. As we discussed in our meeting on August 24, 2017, I want to share with you additional information regarding the recommendations contained in this audit report.

Recommendation: Obtain and Retain an Information Security Officer (ISO)

As reported, the ISO position has been a challenge to keep filled. The compensation that is required for this position, as well as the competitiveness of the industry, have combined to make it difficult to retain an ISO. Nonetheless, we have continued to make progress with information security. As listed in this audit, we have made satisfactory progress with two of the findings in the 2013 APA report. We have updated policies, completed risk assessments, business impact analysis documents, continuity of operations plans, and disaster recovery plans. On August 7, 2017, a qualified, full-time Information Security Officer began employment in the Office of the Executive Secretary. She will work closely with OES staff to refresh the information security program and ensure compliance with state information security standards. We are also in discussions with key partners to develop proposals to advance our information security program.

Recommendation: Improve Disaster Recovery Controls

We recognize the need to improve the disaster recovery controls identified in this finding. We have received and have evaluated proposals from various providers for such services. In prior fiscal years, we have sought funding to procure the identified controls, but this has not yet been funded. We will continue to work with the General Assembly to seek funding for this critical control. While we do not yet have funding to completely mitigate this risk, we do have plans in place to minimize the exposure as much as possible.

Recommendation: Continue to Improve Sensitive Systems Risk Assessment and Contingency Planning Documentation

As identified in this audit, the lack of continuity in the ISO position has hampered our ability to build out the information security program to our satisfaction. However, we have applied resources at various levels to ensure that the information maintained by OES is secure. During development and prior to deployment, applications are tested for vulnerabilities via the use of vulnerability discovery tools. We also maintain a complex array of Intrusion Detection/Prevention systems, network traffic analysis tools, anti-malware tools, and endpoint protection tools to secure our network, data, and applications. We also engage in annual unannounced vulnerability testing engagements with third-party providers to get an outsider's view on our network security posture. We have consistently performed well with these testing engagements.

The FY 2013 audit occurred while we were engaged with a consulting firm to update OES' Business Impact Analysis (BIA), Risk Assessments (RA), Continuity of Operations Plan (COOP), and Disaster Recovery (DR) plan. Updates to these documents occurred in 2007, 2010, 2014, and we are currently in discussions with consulting firms to update these plans in 2017. Since 2014, SEC 501 has changed substantially and these new requirements will be included in the 2017 versions of the BIA, RA, COOP, and DR plans.

Recommendation: Continue Improving Database Security

As identified in this Audit, the lack of continuity in the ISO position has hampered our ability to build out the information security program to our satisfaction. However, we have applied resources at various levels to ensure that the information maintained by OES is secure. Due to budgetary constraints, a replacement centralized security information and event management (SIEM) solution was delayed and not procured until FY2016. This new solution has replaced the previous log management tool and is installed and actively gathering log information from a plethora of sources. We are currently working with the solution provider to customize and fine-tune the solution to fit our needs and the needs identified in SEC 501.

Recommendation: Maintain Oversight of Third-Party Service Providers

As identified in this audit, the lack of continuity in the ISO position has hampered our ability to build out the information security program to our satisfaction. However, we have applied resources at various levels to ensure that the information maintained by OES is secure. SEC 525 was initially published in March 2016 and, while the written policies mentioned in this management point are not yet developed, the process is in place. In FY 2016, OES had one external service provider and the OES IT Director and network engineer reviewed the Service Organization Control 2 (SOC-2) compliance report for this provider.

Now that an ISO is in place, development of these policies will be completed.

Recommendation: Perform Information Technology Security Audits

As identified in this audit, the lack of continuity in the ISO position has hampered our ability to perform IT security audits. However, we have applied resources at various levels to ensure that the information maintained by OES is secure. During development and prior to deployment, applications are tested for vulnerabilities via the use of vulnerability discovery tools. We also maintain a complex array of Intrusion Detection/Prevention systems, network traffic analysis tools, anti-malware tools, and endpoint protection tools to secure our network, data, and applications. We also engage in annual unannounced vulnerability testing engagements with third-party providers to get an outsider's view on our network security posture. Our recently hired information security officer will be tasked with identifying information security providers to assist with development and execution of these audits.

Recommendation: Perform a Risk Analysis for Exceptions to the Acceptable Use Policy

As identified in this audit, the lack of continuity in the ISO position has hampered our ability to build out the information security program to our satisfaction. The Acceptable Use Policy has been rewritten to remove the broad exclusion written into the current version. The proposed policy also includes an exception process as outlined in SEC-501. This version is currently under review by the Court and we await approval before publishing. Additionally, the new ISO is reviewing the proposed policy changes for any additional changes needed to bring the policy into compliance with SEC-501.

If you need any additional information, please do not hesitate to contact my office.

With best wishes, I am

Very truly yours,

Karl R. Hade

cc: John B. Rickman
Robert L. Smith

OFFICE OF THE EXECUTIVE SECRETARY OF THE SUPREME COURT OF VIRGINIA

As of June 30, 2016

The Honorable Donald W. Lemons, Chief Justice

Karl R. Hade, Executive Secretary