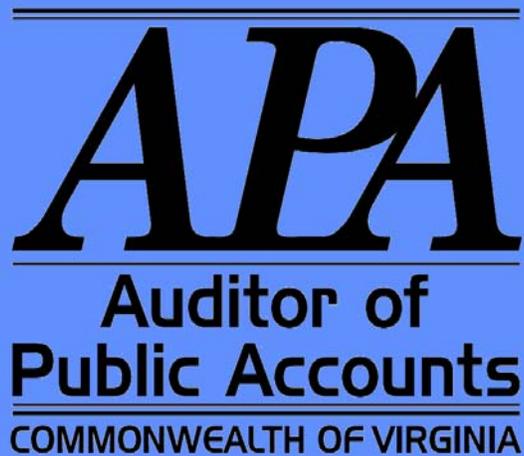


**REVIEW OF  
THE SUPREME COURT'S  
SYSTEMS PLANNING AND OPERATIONS**

**REPORT ON AUDIT  
AS OF  
AUGUST 30, 2007**



## **AUDIT SUMMARY**

Before the Information Technology Department undertakes new projects funded by the Court Technology Fund, they should ensure that the project supports the strategic direction of the Supreme Court and that they manage these projects using formal project management processes. The Information Technology Department needs to work with management of the Supreme Court to provide an information security environment that adequately addresses several areas we believe need improvement, such as their business impact analysis, risk analysis, continuity of operations and their incident response procedure.

Below are some of our recommendations.

- We recommend that as the Supreme Court updates its strategic plan the Department ensure that its IT plan supports all of the Supreme Court's strategies. This approach will help the Department modernize the systems and reduce inefficiencies in the courts system. We also recommend the Department's plans consider how to effectively spend their CTF money.
- We recommend that the Department establish and follow industry best practices for managing IT projects. Although not required to, the Department may wish to adopt and follow Virginia Information Technologies Agency's Project Management Standard since this standard mirrors industry best practices.
- We recommend the Chief Justice of the Supreme Court establish a plan to work with circuit court clerks on creating data standardization guidelines including critical data for information sent to other state agencies as necessary.
- We recommend that the Department document and implement an incident response plan in accordance with industry best practices. We recommend that the Department ensure that IBM develops and documents a business impact analysis and risk assessment that will be beneficial to the Department and its IT environment. We also recommend that the Department continue their plans for a formal security awareness and training program in accordance with industry best practices.

There are other recommendations in our report.

- TABLE OF CONTENTS -

	<u>Pages</u>
AUDIT SUMMARY	
REASON FOR AUDIT	1
OBJECTIVES AND METHODOLOGY	1
DEPARTMENT BACKGROUND	1-2
INFORMATION SYSTEMS STRATEGIC PLANNING AND DEVELOPMENT	2-5
INFORMATION SYSTEMS SECURITY	5-8
DEPARTMENT EFFICIENCIES	8-9
INDEPENDENT AUDITORS REPORT	10-11
AGENCY RESPONSE	12-20

## **REASON FOR AUDIT**

The Supreme Court of Virginia does not fall under the supervision of the Virginia Information Technologies Agency (VITA), like other judicial, legislative, independent branch agencies and institutions of higher education. Although these agencies are exempt from VITA's policies, procedures and standards, they must still provide for sound internal controls over information technology (IT) through the adoption of and compliance with policies and procedures that meet industry best practices. The purpose of our audit is to understand and compare the Supreme Courts Information Technology Department's (Department) policies and procedures to industry best practices.

## **OBJECTIVES AND METHODOLOGY**

Our audit reviewed the Department's IT policies and procedures in five areas as described in the following audit objectives.

1. To determine if the Department's IT strategic plan is in alignment with their overall strategic plan and effective for long-term growth.
2. To determine if the proper oversight and management exists for IT projects, both internally and at Circuit Courts throughout the Commonwealth and whether industry best practices are used throughout the Department.
3. To determine if the Department has documented, approved, and implemented an IT Security Program that provides adequate controls over their information technology resources and data and complies with industry best practices.
4. To follow-up on findings from our office's Statewide Review of Information Security in the Commonwealth conducted in Fall 2006.
5. To analyze the Department for any operating inefficiencies that may exist.

We conducted this audit by interviewing the Department's IT Director and his staff on several occasions. We also requested and reviewed policies, procedures and sampled documents throughout our audit to determine if the Department followed industry best practices. We used the Project Management Institute's Project Management Body of Knowledge (PMBOK), Control Objectives for Information and Related Technology (COBIT) and the International Organization for Standardization (ISO) as industry best practice sources.

## **DEPARTMENT BACKGROUND**

The Department maintains several major IT systems used throughout the Commonwealth's court system including a Case Management System (CMS), Financial Management System (FMS) and Record Management System (RMS) and Magistrates System, and we describe these systems in more detail later in this report. They also have the following responsibilities:

- Provide day-to-day support to over 5000 system users.
- Develop information system test plans and test criteria.

- Procure, install, and maintain telecommunications networks and WAN/LAN environments throughout the Commonwealth.
- Develop, implement and maintain all systems software.
- Safeguard tape and disc libraries.
- Procure, install, and support personal computer hardware, software and peripherals.
- Procure, install, and support all server hardware, software, and peripherals including the Judicial Internet and Intranet.
- Implement, support, and maintain human resource applications.
- Provide support and assistance on systems and automated applications-related projects to the Office of the Executive Secretary and the Judiciary.

The Department implements, maintains, and administers standardized uniform automated systems and the majority of the computer applications in support of the Virginia Judicial System which consists of over 5000 users. The Department consists of approximately 90 employees, of which 27 are contractors. The Department has a budget of approximately \$17.6 million for fiscal year 2007. The Fiscal 2007 budget includes contractor expenses, but excludes personnel costs.

The Department's Director has responsibility for strategic-level technology planning for the Judicial Branch, and the day-to-day management and operation of the Department. The Director oversees the functions performed by the Field Services, Computer Operations, Technical Services, Network Applications, Applications Development, and Administrative divisions.

### **INFORMATION SYSTEMS STRATEGIC PLANNING AND DEVELOPMENT**

In January 2007 the Commission on Virginia Courts in the 21<sup>st</sup> Century created recommendations for the Supreme Court to consider in their overall strategic plan for the Courts in the Commonwealth. The Commission released this report to the public; however, the Supreme Court has not officially adopted any of the recommendations into their strategic plan. The report describes initiatives that the judiciary should undertake and it serves as a guide for the court system in many areas including information technology. To date the Supreme Court has not updated its 2003-2006 strategic plan and does not plan to do so until the Commission's recommendations are finalized.

The Supreme Court's most recent strategic plan is for the period 2003-2006, but it does not address any periods beyond 2006. As the Supreme Court, considers the Commission's recommendations in developing its strategic plan for 2008 and beyond, it needs to fully consider the direction it wants IT to take in supporting the future plan.

Fundamental to achieving any strategic plan is the development and execution of an IT strategic plan that aligns with and supports the Supreme Court's strategic plan. However, the Department does not have such a plan for addressing its overall supporting role to the Supreme Court's goals and therefore there is a high risk of not achieving the goals.

Historically the Department has had limited funds available for major improvements or development efforts to their systems. Funding limitations have had the Department concentrating on IT maintenance projects and hardware with minimal new systems development efforts.

However, the Department recently began receiving information technology funding through the newly created court's technology fund (CTF). In 2006, legislation passed establishing the Court Technology Fund as a special non-reverting fund administered by the

Supreme Court. The Department allocates money in the CTF to projects for the purpose of contractor staffing, advancing, updating, maintaining, replacing, repairing and supporting the telecommunications and technology systems. In 2006 this fund contained approximately \$6 million and in 2007, expects to collect \$8.1 million.

The Department is lacking detailed documented plans and strategies on how they will use the CTF or their normal budget funds. In the past this would not have been a big concern due to the lack of money available to develop new systems, but now with the CTF funds and the Commission's strategic plan, having an IT strategic planning is essential to ensure the Department use the funding to support the Commission's goals and objectives.

If the Department had a detailed plan, they could better ensure that the CTF funds supported priority projects and made the most efficient use of the funds. Since most of the current court systems are antiquated and require replacement, it is imperative that the Department establish and maintain an IT strategic plan to provide accountability for spending the CTF while simultaneously achieving the Supreme Court of Virginia's goals.

**Recommendation 1**

We recommend that as the Supreme Court updates its strategic plan the Department ensures that its IT plan supports all of the Supreme Court's strategies. This approach will help the Department modernize their systems and reduce inefficiencies in the courts system. We also recommend the Department's plans consider how to effectively spend their CTF money.

Systems maintenance projects are a large portion of the Department's IT work; however, they do not have the ability to quantify the dollars spent on each project. The Department does not have a strong project management system or process as discussed below. In the past this lack of a strong project management system or process was not a significant concern due to the limited money available to develop new systems. But with the availability of CTF funds, strong project management is essential to ensure proper planning and management of projects to support the IT strategic plan and ultimately the Supreme Court of Virginia's goals.

The Department does not account for the actual cost of IT development projects; this is a symptom of its lack of a strong project management system and process. We reviewed their IT policies and procedures and interviewed several members of IT management regarding their systems development practices. Several areas of concern that we noted include the following.

- Not tracking the costs involved with systems development projects, primarily internal resource costs.
- Lack of formal training plans for inexperienced project managers managing projects.
- Lack of formalized process in developing systems.
- Missing core project documentation:
  - Charter
  - Budget
  - Key milestone deliverable dates
  - Risk analysis
  - User acceptance criteria
  - Issues tracking
  - Cost-Benefit Analysis

The Department does not have formal guidelines and procedures for systems development projects. The Project Management Institute's Project Management Body of Knowledge (PMBOK) provides structured phases as well as expectations for deliverables that should occur during each phase. These guidelines help give project managers the best possible framework for a successful system implementation, and have proven essential to managing projects effectively.

The Department also has no formalized project development methodology, which includes documenting the project via a charter, formal requirements gathering and documentation, and change controls to manage project scope. These are key components and recognized as best practice in the project management industry.

**Recommendation 2**

We recommend that the Department establish and follow industry best practices for managing IT projects. Although not required to, the Department may wish to adopt and follow VITA's Project Management Standard since this standard mirrors industry best practices.

The Department also does not provide any of its staff formal project management training. Those who lead projects are doing so because they are the team leader, not because they are experienced project managers who have received formal project management training. Not having training or a project management background also makes it difficult to be successful in managing projects.

**Recommendation 3**

We recommend the Department require their project managers to attend a project management classes to give them the tools and knowledge to effectively manage systems development projects. These classes are available through the Commonwealth at reasonable rates.

The Auditor of Public Accounts issued a report in September 2006 discussing the systems development activities at the 120 circuit court clerk's offices throughout the Commonwealth. (*Virginia Circuit Court Systems*, available on-line at [www.apa.virginia.gov](http://www.apa.virginia.gov)). The report discussed the three core systems the Department provides and that the majority of the courts in the Commonwealth use. They are the Case Management System (CMS), Financial Management System (FMS) and Records Management System (RMS). These systems record revenues of approximately \$2 billion annually, and track cases and land records respectively.

However there are several circuit court clerks, approximately 3, that have purchased or developed their own financial or case management systems. These systems do not interface with the Department, which therefore does not allow data transfer to key agencies in the Commonwealth, such as the Department of Motor Vehicles (DMV), The Department of Taxation (TAX) and the Virginia State Police (VSP).

Although there is a minority of the clerks not using the Department's systems, there is the potential for several other clerks to sever their connections to the Departments systems. This potentially will lead to all 120 circuit court clerks buying and maintaining their own non-Department interfacing systems. These actions could lead to duplicative systems and the inefficient use of state and local funds.

Our report recommended that the Chief Justice use his authority over these clerks to require the courts to use the Department's systems in an effort to reduce money spent on duplicative system efforts across the 120 circuit court clerks or the Chief Justice establish system standards which independently developed system must meet. Clerks have continued to develop systems that meet their local needs and do not interface critical data with other state agencies, such as State Police, Tax and the Department of Motor Vehicles, which are critical to reporting items such as delinquent fines and arrest warrants.

**Recommendation 4**

We recommend the Chief Justice of the Supreme Court establish a plan to work with circuit court clerks on creating data standardization guidelines including critical data for information sent to other state agencies as necessary.

**INFORMATION SYSTEMS SECURITY**

In 2006, the Auditor of Public Accounts conducted a Statewide Review of Information Security in the Commonwealth to evaluate the adequacy of the security of state government databases and data communications. The Commonwealth's agencies and institutions of higher education completed a checklist that consisted of a series of detailed questions concerning the existence of written information systems security polices and procedures based on industry best practices.

An effective Information Technology Security Program includes policies and procedures that provide reasonable assurance that appropriate levels of confidentiality, integrity and availability exist to protect and secure IT Systems and the data stored within them. The Statewide Review of the Information Security Checklist submitted in 2006 by the Department demonstrated that the Department lacks or needs improvement in several key components of an adequate Information Technology Security Program, including the following components.

- Designation of IT Security Roles and Responsibilities
- Formal Security Awareness and Training Program
- Business Impact Analysis
- Risk Assessment
- Continuity of Operations Plan
- Disaster Recovery Plan
- Logical Access Controls
- Incident Response Plan

A follow-up on the Statewide Review of Information Security shows that the Department has entered into a contract with IBM to develop and document a Business Impact Analysis and Risk Assessment. The proposed delivery date on these documents was August 30, 2007. In addition, the Department is evaluating an interactive, web-based solution from Awareity, Inc. for their formal security awareness and training program.

Awareity produces a comprehensive toolkit for security awareness training known as Managed Ongoing Awareness Tools (MOAT). VITA also uses the MOAT product to meet their security awareness training requirements set forth in their Information Technology Resource Management standards. Although not required to comply with the standards established by VITA, the Department's security awareness training will be consistent with that of VITA.

**Recommendation 5**

We recommend that the Department ensure that IBM develops and documents a Business Impact Analysis and Risk Assessment that will be beneficial to the Department and its IT environment. We also recommend that the Department continue their plans for a formal security awareness and training program in accordance with industry best practices.

In order to define IT security measures and access controls, the Department needs to establish a security management structure by appropriately assigning IT security roles and responsibilities. This structure should include those program managers who are responsible for the day-to-day reliability and integrity of the IT systems and data.

The Department recently designated an Information Security Officer; however, this individual cannot assume sole responsibility for the management and protection of the IT systems and data. Management of the Supreme Court also needs to assign and establish the roles of data owner, system owner, data custodian, system administrator and system users and their responsibilities, including ownership of the various computer resources and related data.

Once Management has assigned ownership, management also needs to work with various groups to firmly establish the level of sensitivity of these resources and data. Accordingly, the controls to access resources and data should consider one's need to know and job function. Further, information systems security polices should determine who needs to monitor compliance with established policies and procedures. Finally, management will want to make sure that all responsibilities have appropriately segregated duties to reduce the risk of unintentional misuse of the IT systems and data.

**Recommendation 6**

We recommend that the Department appropriately assign the IT security roles and responsibilities in accordance with industry best practices.

An effective Continuity of Operations Plan (COOP) minimizes the probability and impact of a major IT service interruption of essential business functions and processes. This plan should have sufficient documented details that its success does not depend on the knowledge and expertise of a few individuals.

To satisfy this level of detail and to ensure continuation of operations during an IT interruption, the Department should document detailed manual processing procedures for essential business functions that staff can follow until restoration of normal operations. To support these essential business functions and restore the critical applications, the recovery requirements should also document the IT systems and data. The Department has developed a basic COOP that provides guidance for the continuation of mission essential administrative functions and a separate COOP for the continuation of IT operations; however, if the Plan is to be effective, the Department must coordinate these activities.

**Recommendation 7**

We recommend that the Department enhance their COOP by including detailed manual processing procedures for essential business functions that staff can follow until restoration of normal operations occurs. The plan should meet the requirements of industry best practices.

**Recommendation 8**

We recommend that the Department enhance their COOP by including the recovery requirements for those IT systems and data that support the essential business functions in the event of an emergency and by assigning an IT employee to collaborate with the COOP Coordinator in accordance with industry best practices.

To ensure the security on a daily basis, the Department should document, implement and enforce its logical access controls to IT systems and data. The Department's logical access control policies including account management, password management and remote access policies, are general and lacking in detail.

Logical access controls provide a level of assurance against unauthorized and inappropriate modification or disclosure of the Department's IT systems and data against unauthorized and inappropriate modification or disclosure by limiting users' access to computer resources and data. Logical access controls should include the enforcement of strong, complex passwords for all accounts used to access the Department's computer resources and data. Logical access controls should also promote security by requiring the use of encryption for remote access of the Department's computer resources and the transfer of sensitive data.

**Recommendation 9**

We recommend that the Department enhance the logical access control policies for their IT Systems and data in accordance with industry best practices.

The Department is increasing the interconnectivity of its IT Systems; therefore security incidents have the potential to place many valuable computer resources and information at risk for corruption, misuse, or disclosure. A well developed Incident Response Plan can assist the Department in containing and repairing damage from security breaches and preventing future breaches. The Department should document its formal incident response procedures and make their IT system users aware of these procedures and how and when to make use of them through a security awareness training program.

**Recommendation 10**

We recommend that the Department document and implement an Incident Response Plan in accordance with industry best practices.

The Department's Policy and Procedures Memoranda for its IT Systems Development Live Cycle (SDLC) do not include security requirements and controls within the systems development methodology. The IT SDLC should ensure that IT system projects comply with established IT security policies, legal and regulatory requirements, and business requirements for security. IT security considerations should be part of the definition of system requirements, the analysis and design phases, testing processes, and implementation phase and system disposition.

The need to identify SDLC security requirements and controls will become increasingly more important as the Department continues development of web-based applications.

**Recommendation 11**

We recommend that the Department include security requirements and controls in their IT Systems Development Life Cycle in accordance with industry best practices.

The Statewide Review of Information Security follow-up and the additional review of the IT Systems security environment reveals that the Department does not have adequate IT security policies and practices in place to properly safeguard its critical IT assets and data. The Department's core IT security policies, processes and procedures are missing, outdated or not sufficiently detailed to be effective. Inadequate IT security policies diminish the Department's ability to provide assurance that their IT Systems are secure and that the data stored within them are reliable and accurate.

**DEPARTMENT EFFICIENCIES**

The Department supports approximately 5000 users across the Commonwealth on their many systems. They receive calls for technical support regularly, approximately 300 per day; however, they do not have a central help desk number for users to call seeking help. Users call the computer room, where a computer operator takes the call and either helps the user or sends their request on to the appropriate IT staff for assistance. Staff manually route calls and there is no log to assist the Department in tracking help desk inquiries and problem resolution.

Not having a central number nor a central system to record/monitor the calls can cause calls to be lost in the "shuffle" or require a solution that's previously been determined by another IT staff, but went unknown due to it not being documented. Not having a tracking system also leads to the inability to analyze systems and their weaknesses with respect to repetitive help requests. With the Department re-writing several of their systems, the help desk call volume will most likely rise as people learn and adapt to the newer, more modern systems.

**Recommendation 12**

We recommend that the Department establish a central help desk phone number to allow users to call one central location for help requests. We would also recommend that the Department implement a process to track help requests and their solutions, which should help point out areas that need work and/or extra training to the users.

The Department has chosen to not track the financial status of their systems development projects nor do they document a budget for their projects and/or programs. The only costs they can provide are those costs paid vendors. However, to completely cost a systems development project, the Department needs to capture their internal staff's salaries and other Department overhead. This is especially important since there is a large number of systems development project work performed internally by staff within the Department

We also discovered that the Department provides a Record Management System (RMS) to the majority of circuit courts that request this service. The Department acts in a vendor capacity in that they charge the circuit courts for this service. After reviewing the Department's budget we determined that the RMS program area is not recovering costs by not charging a

sufficient fee to cover the cost of providing the service. This situation resulted from the Department's decision not to charge their actual internal resource costs associated with the RMS service to the local courts. The Department can easily quantify the hardware and software costs, but they have made the decision to not charge local courts for the Department's internal resource costs. In the fiscal year 2007 the Department billed the circuit courts approximately \$1 million, however this revenue is insufficient to cover the expenses of the RMS program area, which resulted in unrecovered costs of approximately \$335,000.

**Recommendation 13**

The Department should formalize a process to track budgeted and actual costs for their IT projects and programs. They should establish minimum criteria for tracking all project costs.



# Commonwealth of Virginia

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

Walter J. Kucharski, Auditor

August 30, 2007

The Honorable Timothy M. Kaine  
Governor of Virginia  
State Capital  
Richmond, Virginia

The Honorable Thomas K. Norment, Jr.  
Chairman, Joint Legislative Audit  
and Review Commission  
General Assembly Building  
Richmond, Virginia

We have completed an audit of the Supreme Court's information technology environment and are pleased to submit our report entitled "Review of the **Supreme Courts Systems Planning and Operations.**" We conducted our audit in accordance with the standards for performance audits set forth in Government Auditing Standards, issued by the Comptroller General of the United States.

We had five objectives for our review of Virginia Supreme Court's Systems. These objectives sought to determine:

1. If the Department's IT strategic plan is in alignment with their overall strategic plan and effective for long-term growth.
2. If the proper oversight and management exists for IT projects, both internally and at Circuit Courts throughout the Commonwealth and whether industry best practices are used throughout the Department.
3. If the Department has documented, approved, and implemented an IT Security Program that provides adequate controls over their information technology resources and data and complies with industry best practices.
4. Follow-up on findings from our office's Statewide Review of Information Security in the Commonwealth conducted in Fall 2006.
5. To analyze the Department for any operating inefficiencies that may exist.

Our audit provides several recommendations for Supreme Court to improve internal controls and agency oversight relative to information technology and project management. These recommendations are discussed throughout the report and in our executive summary.

Exit Conference and Report Distribution

We met with management and discussed the report on August 30, 2007. Management's response has been included at the end of this report.

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

WJK:clj

# SUPREME COURT OF VIRGINIA



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

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

HISTORICAL COMMISSION  
MELINDA LEWIS, DIRECTOR

HUMAN RESOURCES  
JOHN M. CARTER, DIRECTOR

JUDICIAL INFORMATION TECHNOLOGY  
ROBERT L. SMITH, DIRECTOR

JUDICIAL PLANNING  
CYRIL W. MILLER, JR., DIRECTOR

JUDICIAL PROGRAMS  
KARL A. DOSS, DIRECTOR

JUDICIAL SERVICES  
PAUL F. DELOSH, DIRECTOR

LEGAL RESEARCH  
STEVEN L. DALLE MURA, DIRECTOR

LEGISLATIVE & PUBLIC RELATIONS  
KATYA N. HERNDON, DIRECTOR

September 13, 2007

Mr. Walter J. Kucharski  
Auditor of Public Accounts  
James Monroe Building  
101 North 14<sup>th</sup> Street  
Richmond, Virginia 23219

Dear Mr. Kucharski:

Thank you for the opportunity to comment on the recent audit report draft titled, "Review of the Supreme Court's Systems Planning and Operations," dated August 30, 2007. Chief Justice Leroy Rountree Hassell, Sr., and I have reviewed the report with the Director of the Supreme Court's Judicial Information Technology Department and other appropriate staff. I have responded below to each of your recommendations.

## **Recommendation 1**

We recommend that as the Supreme Court updates its strategic plan the Department ensures that its IT plan supports all of the Supreme Court's strategies. This approach will help the Department modernize their systems and reduce inefficiencies in the Court's system. We also recommend the Department's plans consider how to effectively spend their CTF money.

During 2005, the Chief Justice established the Commission on Virginia Courts in the 21<sup>st</sup> Century: To Benefit All, To Exclude None. The Commission's recommendations will provide the foundation for the next Judicial System Strategic Plan. The Commission completed its work in 2006 and presented its final report to the Chief Justice in January of 2007. The report was subsequently distributed to every judge in the Commonwealth for his or her review and comment. This fall, the report will be presented to the Judicial Council of Virginia for a vote on each recommendation. Judicial Council's recommendations will then be presented to the Supreme Court of Virginia. The recommendations adopted by the Supreme Court will become the major components of the new strategic plan, which will be released July 1, 2008.

Prior to this strategic planning effort, the Supreme Court of Virginia made the decision to extend the existing Judicial System Strategic Plan. Throughout this process, the Office of the Executive Secretary (OES) has continued to perform its annual comprehensive and operational

planning activities that support the current strategic plan. During the past year, the OES has re-examined its approach to strategic and comprehensive planning to make improvements to both the process and the automated system used to track project activity. The information technology (IT) component has been and will remain a major part of the overall judicial system strategic plan.

The Supreme Court's Technology Fund (CTF) became effective July 1, 2006. The CTF was created to provide an ongoing funding source to enable the Department of Judicial Information Technology (DJIT) meet critical needs in maintaining a reliable infrastructure, modern system architecture and current systems development platform for the major applications that have been developed to support the Judicial Branch. In his 2005 State of the Judiciary Report, the Chief Justice highlighted plans to use the CTF in Fiscal Year 2006 – 2007 to:

1. Shorten the replacement cycle for personal computers.
2. Increase bandwidth to improve response time and to support additional services.
3. Improve the reliability of the judicial network.
4. Enhance network security.
5. Acquire new video conferencing units and expand the use of video conferencing in the courts.
6. Implement electronic filing in the courts.

Based on the revenue projection for the first year of the CTF, the DJIT Director and Executive Secretary developed a plan to support the goals outlined by the Chief Justice for Fiscal Year 2006 – 2007. This spending plan was reviewed with the Chief Justice and progress was reviewed at monthly meetings between the Executive Secretary and the DJIT Director. The plan will strengthen the judicial information systems infrastructure to ensure that the necessary components will be in place to begin modernization of our legacy Case and Financial Management Systems. Significant progress towards these goals was made during Fiscal Year 2006 - 2007. The Supreme Court of Virginia was able to upgrade its mainframe processing capacity, replace over 1000 PCs, increase network bandwidth, improve network reliability, install new video conferencing units, make system software upgrades required for future application development, and establish a committee to begin designing a statewide electronic filing solution.

**Recommendation 2**

We recommend that the Department establish and follow industry best practices for managing IT projects. Although not required to, the Department may wish to adopt and follow VITA's Project Management Standard since this standard mirrors industry best practices.

DJIT has developed and maintains enterprise Case Management and Financial Management Systems for all district courts and most of the circuit courts throughout the Commonwealth. Additionally, the department has developed and maintains a statewide e-Magistrate system and a Records Management System that is used by 75 of the 121 circuit courts throughout

the state. These applications were developed in accordance with the following DJIT policies and procedures:

1. PPM-007 – Automated System Testing
2. PPM-201 – Service Request Processing
3. PPM-202 - Operations/Applications Systems Problem Reports
4. PPM-601 - System Development Life Cycle Methodology (SDLCM)
5. PPM-901 – Change Request Processing

DJIT is in the early stages of a number of major initiatives to rewrite and modernize its legacy applications using Java and IBM's Websphere development platform. These web-based technologies will likely make current development policies and procedures obsolete. As part of this process, DJIT will explore and implement new standards that are compatible with the development methodology of these products and reflect industry best practices.

In January 2006, the OES selected a former Chief Information Officer (CIO) of a Fortune 500 company to fill the Applications Development Manager position. This position was created to oversee and lead the various project teams responsible for the major legacy systems. This position is also responsible for making recommendations to change existing development policies and procedures as the Applications Development Division begins development projects based on the newer web-based technologies.

For re-engineering of these legacy systems, it has been recommended that DJIT use IBM's Rational Unified Process (RUP) methodology. The Rational process is based on the Information Technology Infrastructure Library (ITIL) standards. As legacy applications are rewritten using this methodology, our DJIT project management will mirror industry best practices.

### **Recommendation 3**

We recommend the Department require their project managers to attend a project management class to give them the tools and knowledge to effectively manage systems development projects. These classes are available through the Commonwealth at reasonable rates.

Most of the team leaders within DJIT each have over 20 years of experience developing, maintaining, and managing the critical applications for which they are responsible. In many cases, these team leaders are the original architects of these systems. In response to the increasing demands in managing complex IT applications, the DJIT department was reorganized to create an Applications Development Manager position to oversee the team leaders and their system development staff. The individual selected, a former CIO for a major corporation with an IT department significantly larger than that of the Supreme Court of Virginia, has the experience and expertise needed to assist the department as we begin our major new systems development projects.

The OES agrees that additional project management and technical classes can benefit anyone, regardless of past experience, and enhance overall project management effectiveness.

Therefore, the Director of DJIT will review the courses available through the Commonwealth, as well as the courses available through leading industry training organizations. Once this review is completed, the DJIT Director will recommend courses and course attendees to the Executive Secretary for funding approval.

**Recommendation 4**

We recommend the Chief Justice of the Supreme Court establish a plan to work with circuit court clerks on creating data standardization guidelines including critical data for information sent to other state agencies as necessary.

Currently, 323 of the 326 courts in the Commonwealth use the Case Management and Financial Management Systems developed by the Supreme Court of Virginia's Department of Judicial Information Technology. These automated systems have been in operation for over 20 years. DJIT also developed and maintains an e-Magistrate system that has been installed in every magistrate office in the Commonwealth.

In Fiscal Year 2005 – 2006, over one billion dollars was receipted through the automated Financial Management System. Each day, over one million transactions are processed through our Case and Financial Management Systems. These two enterprise or state-wide systems have provided many benefits and efficiencies for the Commonwealth.

Over the past 20 years, many interfaces have been developed between the Supreme Court systems and the automated systems maintained by other state agencies. For example, when a magistrate completes a warrant in the Supreme Court's e-magistrate system, data can automatically be retrieved from the warrant and entered into the Case Management System with just the entry of the Offense Tracking Number from the warrant. Additionally, critical criminal disposition data is electronically transmitted to the Virginia State Police to update its criminal history database. Traffic disposition data is electronically transmitted to the Department of Motor Vehicles for updating driver history files. Interfaces have been developed with the Department of Taxation to enhance the Commonwealth's capability to collect delinquent court fines and costs. Many other interfaces have been developed to reduce data entry and share information between agencies, such as an electronic interface for transmitting juvenile petitions from the Department of Juvenile Justice to Juvenile & Domestic Relations District Courts, transmission of support order information to the Division of Child Support Enforcement, and transmission of financial data to the Auditor of Public Accounts for annual court audits.

New interfaces and additional system capabilities are being developed to continue to leverage the Commonwealth's investment in our judicial enterprise systems. In addition, the data maintained in our enterprise systems is used for judicial planning purposes, financial forecasting for the General Assembly, and workload analyses for clerks and new judgeship requests.

Currently, only three circuit courts do not use our automated Case Management System and one circuit court does not use our automated Financial Management System. It is our understanding

that one additional circuit court has made the decision to leave our system to purchase a private vendor system with monies from the Technology Trust Fund. The availability of Technology Trust Fund monies makes it possible for other circuit courts to procure individual systems. This creates the potential scenario for many independent and unconnected systems, thereby leading to many incompatible systems. This makes data sharing difficult, undermines the efficiencies provided by a statewide enterprise system and, in the long run, is collectively more costly than operating a statewide system.

The Supreme Court of Virginia shares many of the concerns detailed by the APA in his report, "Virginia Circuit Court Systems," dated September 27, 2006. Rather than focus our limited resources on standards for data exchange with privately developed systems, when currently only three courts are not on the existing enterprise system, the Supreme Court strongly concludes that it should be the sole provider of case management systems in all courts. The Supreme Court also concludes that some of the recommendations in the previously referenced report should be evaluated and appropriate action taken to ensure a strong statewide judicial automated system that meets the needs of all Virginia's courts, as well as our citizens. This APA report has already documented some of the potential problems and increased costs associated with a non-enterprise approach to providing automated services to Virginia's judiciary.

**Recommendation 5**

We recommend that the Department ensure that IBM develops and documents a Business Impact Analysis and Risk Assessment that will be beneficial to the Department and its IT environment. We also recommend that the Department continue their plans for a formal security awareness and training program in accordance with industry best practices.

In June 2007, we began a Business Impact Analysis and Risk Assessment engagement with IBM. IBM is working with the Judicial Information Security Officer (ISO) to coordinate and facilitate these engagements. To date, IBM has completed a facility inspection, interviewed most stakeholders, and distributed surveys to all involved parties. IBM is reviewing these surveys and in October 2007 will present the results of these engagements to OES.

We are finalizing details with representatives from Virginia.gov for the use of Awareness Incorporated's Managed Ongoing Awareness Tools (MOAT) service. Once this agreement is finalized, the Judicial ISO will develop a security awareness program based on the MOAT service. Use of this service will provide an agency-wide program of annual security education and awareness.

**Recommendation 6**

We recommend that the Department appropriately assign the IT security roles and responsibilities in accordance with industry best practices.

The Courts Technology Fund provided the Court with the funding necessary to make significant information security improvements. In 2006, OES contracted with IBM to perform an ethical hacking engagement. Over the course of three days, IBM performed several network hacking

attempts on the judicial network. Virginia's judicial network received high marks, ranking among the top 10 percent of those clients requesting this service, in terms of security protection against hacking attempts. The final ethical hacking report offered several recommendations to enhance network security. DJIT has used these recommendations to adjust, enhance and improve network security. These changes included replacing the e-mail spam filter with an industry leading solution, replacing our intrusion prevention system, and implementing several additional monitoring systems.

In May 2007, in order to increase security awareness, the Executive Secretary appointed a full-time Judicial Information Security Officer. The ISO has been assigned several tasks to complete and the Supreme Court will seek funding for two additional positions to aid the ISO in performing these tasks. This task list includes developing recommendations to respond to both VITA security standards that affect the Judicial Branch, as well as the APA Fall 2006 Statewide Review of Information Security in the Commonwealth. Each security recommendation contained within this report has been included on the ISO task list for completion by the end of this fiscal year.

The ISO has developed a Draft Security Roles and Responsibility document. The Executive Secretary and the DJIT Director are currently reviewing this document.

**Recommendation 7**

We recommend that the Department enhance their COOP by including detailed manual processing procedures for essential business functions that staff can follow until restoration of normal operations occurs. The plan should meet the requirements of industry best practices.

We have contracted with IBM to review and make recommendations for enhancing all COOP and OES business plans. IBM's approach is based on the industry standard Information Technology Infrastructure Library (ITIL) methodology. These steps are identified below:

1. Risk Readiness Assessment
2. Business Impact Analysis
3. Resilience Assessment
4. Resilience Strategy Design
5. Resilience Plan and Procedures development
6. Program and Procedure Validation

Currently, IBM and key players from within the Judicial Branch are engaged in steps one and two of this process. IBM and OES will work through the additional steps that will ultimately result in new COOP and business plans that OES will test and validate. These new plans will include manual processes for essential business functions.

**Recommendation 8**

We recommend that the Department enhance their COOP by including the recovery requirements for those IT systems and data that support the essential business functions in the event of an emergency and by assigning an IT employee to collaborate with the COOP Coordinator in accordance with industry best practices.

The current COOP was developed prior to implementation of the CTF. While the current COOP covers a wide variety of topics, the depth and breadth of the plan was limited greatly by the level of funding available to maintain and implement the plan. The CTF has provided funds that have enabled the OES to procure the IBM services discussed in our response to Recommendation 7. These services will enable us to enhance our COOP and will include IT recovery requirements that support essential business functions.

**Recommendation 9**

We recommend that the Department enhance the logical access control policies for their IT Systems and data in accordance with industry best practices.

PPM-902 governs DJIT's current logical access control policy. This policy follows the philosophy of least privileges, in which an employee is given the least level of access needed in order to do his or her job. Based on requests from the courts, the DJIT's Security Analyst is responsible for assigning system access to the 5,000 court users of the judiciary's enterprise systems. System access requires two levels of authentication and is restricted by court and terminal ID. Enhancing current logical access control policies is on the ISO list of assigned tasks. The timetable for completion of this recommendation is tied to the request for additional ISO staff mentioned in the response to Recommendation 6.

**Recommendation 10**

We recommend that the Department document and implement an Incident Response Plan in accordance with industry best practices.

Incident reports are handled in a variety of fashions. Stolen equipment incidents are reported to the Capitol Police for investigation. Incidents such as computer viruses or PC software problems are documented and resolved by DJIT's Help Desk personnel. Hardware problems are reported to the Computer Room, where calls are placed to the appropriate vendor for onsite resolution. DJIT's Network Team monitors, blocks, and reports all network intrusion attempts. We do, however, recognize the need to more clearly define and consolidate all incident responses. Funding will be sought in the next Session of the General Assembly to support the ISO in implementing this and all information security recommendations within this document. The ISO is currently reviewing various industry best practice Incident Response Plans. Once the ISO completes this review, he will develop a draft plan for review by the Executive Secretary and DJIT Director.

**Recommendation 11**

We recommend that the Department include security requirements and controls in their IT Systems Development Life Cycle in accordance with industry best practices.

PPM-601 governs our legacy application development. Several security requirements exist in the current systems development environment. As an example, security controls for systems that access juvenile data differ from the controls used in the other Case Management Systems.

As we move forward with our re-engineering initiatives utilizing Java and IBM's Rational Unified Process, current security controls will be replaced with controls that comply with industry best practices. The Applications Development Manager and the Information Security Officer are working to develop the requirements that will be incorporated into our Systems Development Life Cycle.

**Recommendation 12**

We recommend that the Department establish a central help desk phone number to allow users to call one central location for help requests. We would also recommend that the Department implement a process to track help requests and their solutions, which should help point out areas that need work and/or extra training to the users.

We strongly believe that a central Help Desk Call Center would benefit the users of the Judicial Branch IT systems. During the 2008 session of the General Assembly, we will request funding for two additional positions to maintain a central Help Desk Call Center.

While we do not currently have these call center positions, we have taken several steps to ensure that our customers have access to DJIT support staff. We have distributed detailed call lists, which include the numbers of all support personnel. In addition, we have provided our users with a "HELP" e-mail account that is monitored by our PC support staff. We have informed all judicial personnel that if they are unsure of which support number to call they can simply send an e-mail to "HELP," and they will receive a call from the appropriate support person. Our Computer Room staff also respond to a variety of support calls. The Computer Room has performed this function for over 20 years, and the telephone numbers for the Computer Room are well known and have not changed during that period.

In 2006, we began implementation of the Magic Inventory System. This system provides a means to track the movement of DJIT equipment through the courts, and provides detailed reporting on what equipment is located in each court and magistrate office. We have also procured the Magic Help Desk System, which will interface with the existing inventory system. Once we have completed the implementation and conversion to the Magic Inventory System, we will begin implementing the Help Desk System. This system will centrally track Help Desk requests and solutions.

Mr. Walter J. Kucharski  
September 13, 2007  
Page Nine

**Recommendation 13**

The Department should formalize a process to track budgeted and actual costs for their IT projects and programs. They should establish minimum criteria for tracking all project costs.

DJIT tracks consultant and hardware/software costs associated with its major IT projects. Although we know our internal IT personnel costs, we have not linked these costs to individual projects because the core function of our internal IT staff is to support the ongoing development and maintenance of the Courts Automated Information Systems. In DJIT, many of the advances made working on one application development project are portable to another. For example, imaging and document capabilities developed for the Records Management System are now being leveraged to provide the same capabilities for our Circuit Case Management System. In addition, these capabilities will one day be integrated with our future electronic filing initiatives. Since the Supreme Court has made the policy decision to develop and maintain mission critical judicial systems in-house and we view our internal IT personnel as resources dedicated to the support of the judiciary, we have concerns over adding this additional level of man-hour accounting to internal systems development projects.

The Office of the Executive Secretary and the Supreme Court of Virginia would like to thank you and your staff for the courtesy and professionalism extended to this office during your review.

With best wishes, I am

Very truly yours,



Karl R. Hade

KRH:sk

