August 2016

Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in the audit of the System of Case and Record Management of the Judiciary

Background

The Missouri Court Automation Committee (MCA), in conjunction with the Missouri Office of State Courts Administrator (OSCA) is responsible for development and implementation of the case and record management system (CRMS) of the judiciary. The OSCA is responsible for providing technical support to Missouri courts and relies extensively on information systems to support mission-related operations and on information security controls to protect the confidentiality, integrity, and availability of sensitive judicial information maintained in those systems. The judiciary relies extensively on the CRMS, including the Judicial Information System (JIS), to process and store court cases, financial information, and other data. The JIS stores personally identifiable information, court cases, financial information, and other data. As of December 2015, the JIS was used by 45 circuits, 3 appellate courts, the Supreme Court, 71 municipal courts, and the centralized Fine Collection Center.

User Account Management

OSCA management has not fully established and documented user account management policies and procedures. OSCA management has not fully established procedures for periodic reviews of user accounts and related privileges to confirm access rights are appropriate. User accounts are not routinely reviewed to determine whether accounts have not been accessed or used for a specified period of time. Additionally, 12 former OSCA or court employees still had access to the JIS after their employment ended. OSCA management also does not require supervisory reviews of system logged actions performed by privileged users or other users with significant access to the network or the CRMS.

Information Security Program

OSCA management has not fully implemented certain elements of an information security program on which security plans, policies, procedures, and controls can be formulated, implemented, and monitored. Weaknesses exist in the information security program that threaten the confidentiality, integrity, and availability of OSCA information and systems. Officials have not established a comprehensive risk assessment and management program or consistently ensured all users are uniquely identified and passwords kept confidential and changed regularly. They also have not established policies to monitor, review, and investigate audit trail records for security and audit related events. Additionally, OSCA management has not fully established an incident response plan for computer security incidents.

System Planning

OSCA management has not fully established some project cost management policies and procedures necessary to minimize project risk. OSCA management has not fully documented the system development life cycle (SDLC) methodology or the policies and procedures for guiding the software development and modification process, including change control management for the system. SDLC is the overall process of developing, implementing, and retiring information systems through a multistep process from initiation, analysis, design, implementation, and maintenance to disposal, according to accepted standards. OSCA management did not prepare project budgets or estimates of project costs for the development, implementation, updating, and maintenance of all system changes required for the CRMS. In addition, OSCA management has not properly accounted for some project costs. OSCA management has not developed a formal long-range plan or prepared adequate estimates of the additional costs expected for the CRMS. A major funding source for the CRMS is the court automation fee established in section 488.027, RSMo. However, this fee will sunset September 1, 2023. A formal long-range plan is necessary to ensure the General Assembly is aware of the state's total potential financial commitment prior to funding new features of the CRMS.

Contingency Planning

OSCA management has documented and informally adopted a business continuity plan; however, the plan has not been formally approved by management, updated, or tested, increasing the risk the plan may not be adequate to support the timely recovery of business functions after the occurrence of a disaster or other significant incident. OSCA management has developed certain contingency plans and implemented basic controls for recovery planning. However, the disaster recovery plan has not been fully established or fully tested to ascertain the effectiveness of recovery procedures. The disaster recovery plan was last updated in May 2014.

Monitoring Reports

Opportunities exist to increase the efficiency and effectiveness of the monitoring performed of activity processed in the CRMS at the local courts. These opportunities to assist the courts could be accomplished through additional monitoring reports or other tools. Examples of the reports not currently available to courts include a report to identify cases disposed with no fees or costs assessed or a report to identify cases exempt from debt collections.

In the areas audited, the overall performance of this entity was **Fair**.*

*****The rating(s) cover only audited areas and do not reflect an opinion on the overall operation of the entity. Within that context, the rating scale indicates the following:

Excellent: The audit results indicate this entity is very well managed. The report contains no findings. In addition, if applicable, prior recommendations have been implemented.

Good: The audit results indicate this entity is well managed. The report contains few findings, and the entity has indicated most or all recommendations have already been, or will be, implemented. In addition, if applicable, many of the prior recommendations have been implemented.

Fair: The audit results indicate this entity needs to improve operations in several areas. The report contains several findings, or one or more findings that require management's immediate attention, and/or the entity has indicated several recommendations will not be implemented. In addition, if applicable, several prior recommendations have not been implemented.

Poor: The audit results indicate this entity needs to significantly improve operations. The report contains numerous findings that require management's immediate attention, and/or the entity has indicated most recommendations will not be implemented. In addition, if applicable, most prior recommendations have not been implemented.

All reports are available on our Web site: auditor.mo.gov