Office of the City Auditor
Kansas City, Missouri

Highlights

Why We Did This Audit

Municipal Court implemented a paperless docketing system in August 2011. System availability is critical to operations since Municipal Court functions from automatic case creation to final disposition are handled through the IMDS Plus system.

Security controls for IMDS Plus are important because of the sensitive information contained in court records. Security weaknesses could result in disruptions of the systems and the unauthorized access, use, disclosure, modification, or destruction of system data.

Our work focused on identifying recommended security practices for criminal justice information systems and comparing identified practices with Municipal Court practices and the REJIS' policies, the IMDS Plus vendor. We did not physically test REJIS' controls.

Background

The city pays almost $1.5 million in annual subscription fees to the REJIS Commission for the use of the REJIS systems, including IMDS Plus.

Municipal court staff access the IMDS Plus system through a private network because the applications and data are stored on REJIS' servers.

For more information, please contact the City Auditor's Office at 816-513-3300 or auditor@kcmo.org.

To view the complete report, go to kcmo.gov/cityauditor and click on Search Audit Reports.

PERFORMANCE AUDIT
Municipal Court Docketing System Security

What We Found

The IMDS Plus system contains criminal justice information that must be protected from the time it is created until it is destroyed. Improper access, dissemination or use of criminal justice information is a class A misdemeanor.

The confidentiality, integrity, and availability of information in the IMDS Plus system could be improved with the adoption of additional recommended security practices.

We found that Municipal Court has not:

- terminated user access to the system in a timely manner;
- performed annual reviews of user access;
- conducted some required fingerprint background checks; or
- provided and documented security awareness training for all appropriate employees and contractors.

REJIS has policies to address most of the recommended security practices to ensure the confidentiality, integrity, and availability of information in the system, but REJIS has not:

- updated its disaster recovery plan;
- finalized its incident response procedures; or
- established an alternate processing site to continue operation in case of a prolonged service disruption.

What We Recommend

Our recommendations include:

- Ensuring user access is removed immediately when user's employment status changes and validating user access annually.
- Identifying contractors and employees who are required to have a fingerprint background check and ensuring the background checks are made.
- Providing and documenting security awareness training to appropriate employees and contractors.
- Developing written policies and procedures to meet federal and state agency criminal justice information security requirements.
- Encouraging REJIS to update and periodically test its disaster recovery plan; finalize its incident response procedure; and establish a geographically removed disaster recovery site.
- Including criteria in future information technology service provider contracts to ensure the confidentiality, integrity and availability of city information is protected.

Management agreed with the recommendations.