

**Performance Audit
Municipal Court
Docketing System Security**

February 2014



**Office of the City Auditor
Kansas City, Missouri**

06-2013



Office of the City Auditor

21st Floor, City Hall
414 East 12th Street
Kansas City, Missouri 64106

(816) 513-3300
Fax: (816) 513-3305

February 26, 2014

Honorable Mayor and Members of the City Council:

This performance audit of Kansas City Municipal Court docketing (IMDS Plus) system security was initiated by the city auditor pursuant to Article II, Section 216 of the city charter. The audit focuses on identifying recommended security control practices for criminal justice information systems and comparing identified practices with Municipal Court practices and the policies of the IMDS Plus system provider (REJIS).

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 system access in a timely manner; performed annual reviews of user access; conducted all of the required fingerprint background checks; and 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.

We make recommendations to the municipal court administrator to meet requirements for the handling of criminal justice information and adopt written policies and procedures to meet established requirements. We also recommend that the director of general services encourage REJIS to update and finalize plans and procedures and adopt recommended practices related to disaster recovery and incident response. In addition, we recommend the director of general services develop criteria for future information technology service provider contracts to protect the confidentiality, integrity, and availability of city information.

We shared a draft of this report with the municipal court administrator and director of general services on January 29, 2014. Their responses are appended. We would like to thank Municipal Court, General Services, and REJIS staff for their assistance and cooperation during this audit. The audit team for this project was Nancy Hunt and Vivien Zhi.

A handwritten signature in blue ink that reads "Douglas Jones".

Douglas Jones
City Auditor

Municipal Court Docketing System Security

Table of Contents

Introduction	1
Objectives	1
Scope and Methodology	1
Background	3
City Contracts with REJIS	3
Municipal Court Docketing System	3
Criminal Justice Information	3
Information Technology Service Providers	3
Findings and Recommendations	5
Not All Recommended Security Practices Are in Place	5
City Needs to Improve Controls and Establish Written Policies	5
Not All REJIS Plans and Procedures Are Up To Date	8
City Needs Standards for Information Technology Service Providers	11
Recommendations	11
Appendix A: Municipal Court Administrator’s Response	13
Appendix B: Director of General Service’s Response	23

Introduction

Objectives

We conducted this audit of Municipal Court’s docketing system security under the authority of Article II, Section 216 of the Charter of Kansas City, Missouri, which establishes the Office of the City Auditor and outlines the city auditor’s primary duties.

A performance audit provides findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria. Performance audits provide objective analysis to assist management and those charged with governance and oversight in using the information to improve program performance and operations, reduce costs, facilitate decision making, and contribute to public accountability.¹

This report is designed to answer the following question:

- Are controls in place to protect the confidentiality, integrity, and availability of information in the Integrated Metropolitan Docketing System (IMDS) Plus system?

Scope and Methodology

Our review focuses on reviewing the IMDS Plus system security controls. Our audit methods included:

- Interviewing Municipal Court and Regional Justice Information Service (REJIS) staffs to understand their practices and policies related to the security of the IMDS Plus system.
- Reviewing the FBI’s *Criminal Justice Information Services (CJIS) Security Policy* to identify criteria and recommended practices related to system security.

¹ Comptroller General of the United States, *Government Auditing Standards* (Washington, DC: U.S. Government Printing Office, 2011), p. 17.

- Reviewing the National Institute of Standards and Technology's *Recommended Security Controls for Federal Information Systems*; the United States Government Accountability Office's *Federal Information System Controls Audit Manual*; and the Information Systems Audit and Control Association's *IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals* to identify criteria and recommended practices related to system security, contingency planning, and disaster recovery planning.
- Comparing Municipal Court's and REJIS' policies and practices to identify recommended practices related to system security and disaster recovery planning.
- Obtaining a list of IMDS Plus system active users to determine whether users had a work-related reason to have access to IMDS Plus.
- Reviewing the executive summary of REJIS' most recent external/internal vulnerability assessment performed by an independent vendor to identify audit findings and interviewing REJIS staff to identify corrective actions taken.
- Reviewing the Missouri State Highway Patrol's Missouri Uniform Law Enforcement System Policy Compliance Review of Municipal Court to identify findings regarding system security and interviewing Municipal Court staff to identify corrective actions taken.

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. No information was omitted from this report because it was deemed privileged or confidential.

Background

City Contracts with REJIS

General Services' Information Technology Division administers the city's contract with the REJIS Commission. 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 Docketing System

Municipal Court implemented the IMDS Plus system in August 2011. The system handles all Municipal Court functions from automatic case creation to final disposition, including electronic scheduling of court dockets, and payments of fines and court costs. The system also interfaces with law enforcement systems for automated warrant entry and cancellation. Although citizens receive a paper ticket for traffic and ordinance violations, the court records are paperless – maintained only in an electronic format. Municipal Court staff access the system through a private network because the applications and data are stored on REJIS' servers.

Criminal Justice Information

Municipal Court IMDS Plus users have access to criminal justice information which includes any information collected by criminal justice entities, including but not limited to the FBI and Missouri State Highway Patrol, and personally identifiable information such as name, date of birth, and social security number. Criminal justice information should be protected from the time it is created until it is destroyed. Improper access, dissemination or use of criminal justice information is a serious issue. Misuse of official criminal justice information is a class A misdemeanor.

Information Technology Service Providers

Cloud computing service providers extend existing information technology capabilities by delivering on-demand computing services via the internet. Application service providers deliver on-demand computing services via a private network or the internet. REJIS delivers software services to Municipal Court via a private network.

Municipal Court Docketing System Security

Findings and Recommendations

Not All Recommended Security Practices Are in Place

The confidentiality, integrity, and availability of information in the IMDS Plus system could be improved by the city's and REJIS' adoption of additional recommended security practices. Municipal Court should terminate former users' system access in a timelier manner; perform annual reviews of user access; complete fingerprint background checks; provide and document security awareness training for employees and contractors; and establish written policies and procedures to help staff meet security requirements. REJIS has not updated its disaster recovery plan; finalized its incident response procedures; or established a disaster recovery site that is geographically removed from its data center. In addition, the General Services Department should establish standards for information technology service providers to address the issues of confidentiality, integrity, and availability of information.

City Needs to Improve Controls and Establish Written Policies

Municipal Court should take steps to address recommended practices established to protect criminal justice information accessed through the REJIS system. The court did not consistently disable access rights for all terminated and transferred IMDS Plus users, perform annual reviews of user access, complete fingerprint background checks, and provide and document security awareness training for all appropriate employees and contractors. The development of written policies could improve the court's awareness and implementation of recommended practices related to system security.

Municipal Court did not consistently disable access rights of terminated and transferred IMDS Plus users. We found instances in which users continued to have access to the system after they no longer had a work-related reason. We obtained a list of IMDS Plus users from REJIS in order to verify each user's employment status. We looked up each individual in PeopleSoft, the city's human resources system, to identify city employees and worked with Kansas City, Missouri Police Department staff to identify police employees. We sent Municipal Court a list of users who were no longer working in Municipal Court, the Law Department, or the Police Department; no longer worked for the city; or were not in PeopleSoft, suggesting that they were not city employees.

After reviewing the list, the court administrator determined that 48 of the 51 users we identified should no longer have system access and removed their access.

According to the FBI's *Criminal Justice Information Services (CJIS) Security Policy*, individuals with access to criminal justice information, which would include IMDS Plus users, should only be given the access needed to perform specified tasks, limiting access to authorized personnel with the need and the right to know.² The policy also requires that identification data be kept current by adding new users and disabling and/or deleting former users.³ In addition, the FBI's policy requires the validation of user accounts at least annually.⁴

To better control IMDS Plus accounts in accordance with the FBI's *Criminal Justice Information Services (CJIS) Security Policy*, the municipal court administrator should ensure that user access is removed immediately when an individual's position or employment status changes and validate IMDS Plus user access annually.

Municipal Court is not following fingerprint background check requirements. The FBI's *Criminal Justice Information Services (CJIS) Security Policy*⁵ requires that individuals who have access to criminal justice information have an initial state of residency and national fingerprint-based background clearance and be rechecked every five years. The Missouri State Highway Patrol uses a more stringent standard requiring fingerprint-based background checks every two years. The background checks are required for employees who access criminal justice information as part of their employment duties and personnel, contractors, and custodial workers with unescorted access to secured areas.

In 2011, a policy compliance review performed by the Missouri State Highway Patrol found that Municipal Court was not in compliance with the background check requirements. Three employees were found to have criminal histories that the court eventually addressed and custodial staff and an employee witnessing the shredding of confidential documents had not had the required background checks.

² *Criminal Justice Information Services (CJIS) Security Policy*, U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, Version 5.2, Section 5.5.2.1 Least Privilege.

³ *Criminal Justice Information Services (CJIS) Security Policy*, Section 5.6.1 Identification Policy and Procedures.

⁴ *Criminal Justice Information Services (CJIS) Security Policy*, Section 5.5.1 Account Management.

⁵ *Criminal Justice Information Services (CJIS) Security Policy*, Section 5.12.1.1 Minimum Screening Requirements for Individuals Requiring Access to CJIS.

Having proper security measures against potential insider threats is a critical component of security. The new municipal court administrator is working with the General Services Department to obtain a list of individuals who have unescorted badge access to Municipal Court.

To ensure all employees, contractors, and custodial workers with unescorted badge access to areas in which criminal justice information could be available have required background checks, the director of general services should work with the municipal court administrator to identify contractors and other city employees who are subject to the required fingerprint background check and ensure that the appropriate background checks are made.

Municipal Court should provide and document security awareness training. The FBI's *Criminal Justice Information Services (CJIS) Security Policy* requires basic security awareness training for individuals who have access to criminal justice information within six months of their initial assignment and every two years thereafter.⁶ City employees and contractors with access to the IMDS Plus system and Municipal Court secured areas are required to sign a security awareness training form every two years, stating that they have read and will abide by the rules and regulations outlined in the security awareness training materials. The security awareness training materials developed by the Missouri State Highway Patrol cover security requirements and emphasize the importance of protecting information.

The FBI's *Criminal Justice Information Services (CJIS) Security Policy* requires that records of security awareness training be documented, kept current, and maintained by an individual responsible for the administration of the criminal justice information system network.⁷ The court administrator is currently working to provide and gather signed security awareness training forms from employees and contractors.

To ensure city employees and contractors with access to the IMDS Plus system and Municipal Court secured areas meet the security awareness training requirements, the municipal court administrator should systematically provide and document security awareness training for appropriate employees and contractors.

Written policies and procedures could help Municipal Court meet criminal justice information protection requirements. Although federal and state agencies have established requirements for the protection of criminal justice information, court staff have not always

⁶ *Criminal Justice Information Services (CJIS) Security Policy*, Section 5.2 Security Awareness Training.

⁷ *Criminal Justice Information Services (CJIS) Security Policy*, Section 5.2 Security Awareness Training.

taken the necessary steps to ensure compliance. Municipal Court does not have written policies and procedures to help it meet requirements regarding granting system access, validating user accounts, disabling user accounts, personnel security for employees and contractors, and security awareness training.

Written policies and procedures can outline the authority and responsibilities of individual employees; serve as a reference tool for infrequently encountered situations; and lessen the threat to continuity posed by employee turnover. Without written policies and procedures, important responsibilities can be overlooked and necessary actions not taken.

Municipal Court's administrative leadership and the employee responsible for overseeing the court's compliance with criminal justice information system policies have been filled by an ever changing list of employees. The court should benefit from the 2013 appointment of a permanent court administrator who has experience and is familiar with the protection of criminal justice information. This appointment should offer stable leadership, strengthen the court's knowledge base, and provide the necessary expertise to develop written policies and procedures to help the court meet established requirements.

To help ensure that security requirements are met, the municipal court administrator should develop written policies and procedures that meet the federal and state agency criminal justice information security requirements.

Not All REJIS Plans and Procedures Are Up To Date

REJIS' policies address most of the recommended practices to ensure the confidentiality, integrity and availability of information in the IMDS Plus system. Additional steps could be taken, however, to further protect the information. REJIS does not have an updated disaster recovery plan, finalized incident response procedures, or an alternate processing site that is geographically removed from its data center.

REJIS has policies to address most recommended security practices.

In evaluating REJIS' controls over the confidentiality, integrity, and availability of information in the IMDS Plus system, we limited our evaluation to a review of REJIS' written policies and followed up with phone interviews with their St. Louis staff. We did not physically test their controls. REJIS did, however, provide and we reviewed the executive summary of REJIS' most recent Internal/External Vulnerability Assessment performed by an independent vendor.

We found REJIS has written policies to address most of the recommended security practices, including:

- Auditing and accountability policies to increase the likelihood of authorized users conforming to a prescribed pattern of behavior.
- Identification and authentication policies to ensure only authorized users can access the system.
- Configuration management policies and practices to allow only qualified and authorized individuals access to system components in order to initiate approved upgrades and modifications.
- Media protection policies to ensure that electronic and physical media are restricted to authorized individuals.
- Physical security policies to ensure criminal justice information and system hardware, software, and media are physically protected.
- Systems and communication policies to secure its virtualized environment and to ensure information integrity.

REJIS has not updated its disaster recovery plan. The REJIS manager of network services security told us the current REJIS disaster recovery plan needs to be modified and updated. Due to security reasons, REJIS provided only four pages of its Disaster Recovery Plan Executive Summary for our review. The January 30, 2007 plan summary states that the “procedures as of this writing are generic in nature” and need to be fleshed out. In addition, the summary states that important disaster recovery decisions related to the purchase of hardware, software, and testing were yet to be made.

Disaster recovery planning is a critical information system general control. Disaster recovery plans set out measures to be followed to increase the speed of operational recovery or better ensure continued operations in the event of a disaster. Because Municipal Court operates in a paperless environment, losing the capability to process, retrieve, and protect electronic information through the REJIS systems would significantly affect Municipal Court’s ability to operate.

Although REJIS told us they had tested their disaster recovery process, REJIS acknowledged that its disaster recovery plan needed to be updated. The testing of an outdated plan would not protect the current availability of system processing and data. Disaster recovery plan testing is essential to determining whether a plan will function as intended in an

emergency situation.⁸ Disaster recovery plans should be tested periodically and the results analyzed and reported to top management so that the need for modification and additional testing can be determined.⁹

To help ensure Municipal Court can continue operating in the event of a disaster, the director of general services should encourage REJIS to update and periodically test its disaster recovery plan.

REJIS' incident response procedures have not been finalized. The FBI's *Criminal Justice Information System (CJIS) Security Policy* requires establishment of an operation incident handling capability for information systems; and the tracking, documenting and reporting of incidents to appropriate officials and authorities.¹⁰ An incident response plan can help the agency to be better prepared when a security incident happens. REJIS' incident response procedure, describing how REJIS will respond to security incidents, was published in draft form in 2008, reviewed in 2012, but is still not finalized.

To respond quickly when a security incident occurs, with procedures and responsibilities identified and set, the director of general services should encourage REJIS to finalize its incident response procedure.

REJIS does not have a geographically removed alternate processing site. The REJIS data center is also the disaster recovery site for REJIS operations in case of a prolonged service disruption. With a single site, natural or man-made disasters such as earthquakes, tornados, telecom and IT system outages, bombs, chemical agents, terrorism, crimes, or pandemics could impact and limit REJIS' access to facilities and operations. Because an alternate disaster recovery site located too close to the primary site of normal operations could cause both to be susceptible to the same hazard, the recommended practice is that an alternate processing site be geographically removed from the primary site.¹¹

To better ensure the continued availability of information stored and processed on the REJIS systems, the director of general services should encourage REJIS to establish a disaster recovery site that is geographically removed from its data center.

⁸ *Federal Information System Controls Audit Manual*, United States Government Accountability Office, February 2009, p. 332.

⁹ *Federal Information System Controls Audit Manual*, pp. 333-334.

¹⁰ *Criminal Justice Information Services (CJIS) Security Policy*, Section 5.3: Incident Response.

¹¹ *Federal Information System Controls Audit Manual*, p. 330 and *Recommended Security Controls for Federal Information Systems*, National Institute of Standards and Technology, December 2007, p. F-31.

City Needs Standards for Information Technology Service Providers

General Services' Information Technology Division should develop city standards for information technology service provider contracts. As the city explores more opportunities to maximize efficiency, including outsourcing operations to application service providers and moving services to the cloud, ensuring the privacy, security, and availability of the data stored outside of the city's network is critical to continued operations. The director of general services should include criteria in information technology service provider contracts to ensure the confidentiality, integrity, and availability of city information is protected.

Recommendations

1. The municipal court administrator should ensure that user access is removed immediately when an individual's position or employment status changes and validate IMDS Plus user access annually.
2. The director of general services should work with the municipal court administrator to identify contractors and other city employees who are subject to the required fingerprint background check and ensure that the appropriate background checks are made.
3. The municipal court administrator should systematically provide and document security awareness training to appropriate employees and contractors.
4. The municipal court administrator should develop written policies and procedures that meet the federal and state agency criminal justice information security requirements.
5. The director of general services should encourage REJIS to update and periodically test its disaster recovery plan.
6. The director of general services should encourage REJIS to finalize its incident response procedure.

Municipal Court Docketing System Security

7. The director of general services should encourage REJIS to establish a disaster recovery site that is geographically removed from its data center.
8. The director of general services should include criteria in information technology service provider contracts to ensure the confidentiality, integrity, and availability of city information is protected.

Appendix A

Municipal Court Administrator's Response



Municipal Court



Date: February 20, 2014

To: Doug Jones, City Auditor

From: Megan Pfannenstiel, Court Administrator 

Subject: Response to Municipal Court Docketing System Security Audit Report

The Municipal Court appreciates the work the City Auditor and his staff performed in completing the audit of the Municipal Court. As more efficiencies are gained with technology, the importance of security around those systems is more important than ever.

Please find my response to recommendations 1, 2, 3 and 4 of the audit as provided below:

1. The municipal court administrator should ensure that user access is removed immediately when an individual's position or employment status changes and validate IMDS Plus user access annually.

Agree. I have created a procedure (Attachment 1) that will ensure access to IMDS Plus and/or any REJIS system is terminated within one (1) week of an employment status change where access to IMDS Plus and/or any REJIS system is no longer needed.

2. The director of general services should work with the municipal court administrator to identify contractor and other city employees who are subject to the required fingerprint background check and ensure the appropriate background checks are made.

Agree. I look forward to working with the Director of General Services on creating formal procedures to identify contractors and/or city employees that need unescorted access to the Municipal Court building. Such contractors and/or employees must not only be fingerprinted but also required to read and sign the Security Awareness Training forms. Attachment 2 documents the procedure the Court will employ to verify appropriate background checks are completed every two (2) years per CJIS requirements.

3. The municipal court administrator should systematically provide and document security awareness training to appropriate employees and contractors.

Agree. I have again created a procedure (Attachment 2) to ensure that security awareness is completed by all individuals that have unescorted access to the Municipal Court building. With this procedure, a log will be kept with all individuals that have such access to the building and the date that they signed the Security Awareness Training

form. This will be reviewed annually to confirm that every person meets the requirement of having the form signed every two (2) years.

4. The municipal court administrator should develop written policies and procedures that meet the federal and state agency criminal justice information security requirements.

Agree. Although not specifically noted in the Audit, the Court has also created a policy for having visitors sign in and out of the secure areas of the Municipal Court building (Attachment 3). I have been working with the Missouri State Highway Patrol and the Kansas City, Missouri Police Department to create additional policies and procedures around system security.

Cc: Troy Schulte, City Manager
Earnest Rouse, Director of General Services

**City of Kansas City, Missouri
Municipal Court**



Standard Operating Procedures – TAC

TITLE: **Granting and Terminating Access to a REJIS System**

PURPOSE:

This SOP is to guide staff assigned as the Terminal Agency Coordinator (TAC) or an Assistant TAC in the steps taken to grant, maintain and terminate access to a REJIS system for Court related purposes under the Court's Originating Agency Identifier (ORI). This is to include access to IMDSPlus, LEWeb, Mobile Ticketing, and CourtWeb. This SOP will also address access to MULES, NCIC, NLETS, DOR and other systems covered by the Missouri State Highway Patrol and the FBI. This SOP does not cover granting access to a REJIS system for other City Departments that have their own ORI.

POLICY:

The Municipal Court is the sole authority with regard to approving, modifying and terminating access to a REJIS system under the ORI MO048051J.

PROCEDURE:

Granting New Access:

Upon hiring or transferring to a position where a person will have access to a REJIS system the person will complete the following steps:

1. The person will complete the appropriate Operator Identification Form (OID) form and provide completed form to the TAC.
2. The TAC will complete a pre-employment criminal history check on the individual. The person must not have any active warrants, felony convictions or pending felony arrests. If the person has active warrants, felony convictions or pending felony arrests, the person will not be approved for access.
3. The TAC will conduct Security Awareness Training for the individual and keep a signed acknowledgement of the training.
4. The TAC will fax the OID form to REJIS and log the person into the REJIS User Spreadsheet notating their access and the date Security Awareness Training was signed.
5. The person will be scheduled to be fingerprinted by the Police Department.
6. The TAC will review the results. If there is a record found but there is not a felony conviction or pending felony arrest, the TAC may review the incident and coordinate with the Court Administrator to determine if access is appropriate. If the Court Administrator feels that access is still appropriate given the criminal history, the TAC may send a letter to the CJIS Systems Officer (CSO) and to REJIS asking permission to grant access. The Court Administrator will make the final determination if access is granted.

Modifying Access:

Sometimes modification of access will be necessary depending upon roles and responsibilities. When this occurs, the following steps must be completed:

1. The supervisor of the operator must notify the TAC of the change in access.
2. The operator must complete a new OID form and provide completed form to the TAC.
3. The TAC must fax the form to REJIS and update the REJIS User Spreadsheet to reflect the changes.

Attachment 1

Terminating Access:

Upon termination or change in employment of an operator, that no longer requires access to a REJIS system, the following steps must be completed:

1. The supervisor of the operator who no longer requires access must notify the TAC as soon as possible, but within seven (7) days of the change in employment status.
2. The TAC, upon notification, must complete an OID form and fax to REJIS.
3. The TAC will update the REJIS User Spreadsheet to reflect date of termination.

**City of Kansas City, Missouri
Municipal Court**



Standard Operating Procedures – TAC

TITLE:	Security Awareness Training
---------------	------------------------------------

PURPOSE:

This SOP is to guide staff assigned as the Terminal Agency Coordinator (TAC) or an Assistant TAC in the steps taken to ensure all individuals who have unescorted access to the Municipal Court Building have completed Security Awareness Training every two years as required by Criminal Justice Information Systems (CJIS) standards.

POLICY:

The Municipal Court is the sole authority with regard to approving and terminating access to the Municipal Court Building. The role of the individual will determine what Security Awareness Training form they will be required to sign.

PROCEDURE:

Granting New Access:

Upon hiring or transferring to a position where a person will have access to the Municipal Court Building the person will complete the following steps:

1. The TAC will complete a pre-employment criminal history check on the individual. The person must not have any active warrants, felony convictions or pending felony arrests. If the person has active warrants, felony convictions or pending felony arrests, the person will not be approved for access.
2. The TAC will conduct the appropriate Security Awareness Training for the individual and keep a signed acknowledgement of the training.
3. The TAC will log the person into the REJIS User Spreadsheet notating their access and the date Security Awareness Training was signed. A separate tab will be used to track individuals who do not have access to a REJIS system but have unescorted access to the Municipal Court Building.
4. The person will be scheduled to be fingerprinted by the Police Department at 901 Charlotte.
5. The TAC will review the results. If there is a record found but there is not a felony conviction or pending felony arrest, the TAC may review the incident and coordinate with the Court Administrator determine if access is appropriate. If the Court Administrator feels that access is still appropriate given the criminal history, the TAC may send a letter to the CJIS Systems Officer (CSO) and to REJIS asking permission to grant access. The Court Administrator will make the final determination of access.

Updating Access:

1. On a quarterly basis at the TAC will review the REJIS User Spreadsheet. Anyone whose training will expire within the next three (3) months, will be recertified. Recertification will require the TAC to run a post-employment criminal background check and have the individual re-read and sign a new Security Awareness Training form.

Terminating Access:

Upon termination of an individual or change in employment that no longer requires access to the Municipal Court Building, the following steps must be completed.

1. The supervisor of the individual who no longer requires access must notify the TAC as soon as possible, but within seven (7) days of the change in employment status.

Attachment 2

2. The TAC will update the REJIS User Spreadsheet to reflect date of termination.

Attachment 2

**City of Kansas City, Missouri
Municipal Court**



Standard Operating Procedures – TAC

TITLE: Unescorted access to secure areas of Municipal Court Building

PURPOSE:

This SOP is to ensure that the Municipal Court Building secure areas comply with all Federal, State and Local CJIS requirements.

POLICY:

Only persons that have been fingerprinted and have a current signed Security Awareness training form on file will be allowed to have unescorted access to the secure areas of the building. All other visitors must sign in and out of the KCMO Municipal Court Visitor's Log.

PROCEDURE

The TAC and/or Assistant TAC will be responsible for maintaining a Visitor's Log on the first floor of the Municipal Court. The log will be kept at the cubicle closest to the conference room. All visitors must sign in and out. Employees are responsible for ensuring their visitors have complied with this procedure. Once a month, the TAC or Assistant TAC will scan the log and file it electronically under the TAC secure folder.

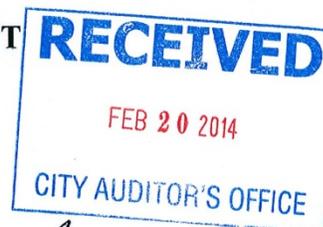
Attachment 3

Appendix B

Director of General Service's Response



GENERAL SERVICES DEPARTMENT



DATE: February 20, 2014
TO: Douglas Jones, City Auditor
FROM: Earnest Rouse, Assistant City Manager/Director of General Services
SUBJECT: Response to Report on Municipal Court Docketing System Security

The City Auditor's Office Report on Municipal Court Docketing System Security is a performance audit of the security of the Regional Justice Information System (REJIS) and its Integrated Metropolitan Docketing System (IMDS Plus) used by the Municipal Court.

The General Services Department is providing this response to specific findings in the audit because two of its divisions, Information Technology and Procurement Services, are integral to the maintenance of the system and the management of the contract between the City and the REJIS Commission.

Please find my response to the audit recommendations as provided below:

- 2. The director of general services should work with the municipal court administrator to identify contractors and other city employees who are subject to the required fingerprint background check and ensure that the appropriate background checks are made.**

Agree. The director of General Services will review contracts and require provisions for background checks and fingerprinting of employees and contractors as required.

- 5. The director of general services should encourage REJIS to update and periodically test its disaster recovery plan.**

Agree. The director of General Services will urge REJIS to update and otherwise modify the disaster recovery plan to ensure that it functions properly in an emergency. Further, the director will ask for a plan that can be periodically tested and analyzed to ensure the integrity of the system and the security of court records.

- 6. The director of general services should encourage REJIS to finalize its incident response procedure.**

Agree. The director of General Services is mindful of the varied threats to electronic systems, whether accidental or intentional, and will encourage REJIS to recognize the importance of proper procedures when such threats or actual incidents occur.

Response to Report on Municipal Court Docketing System Security
February 20, 2014
Page Two (2)

General Services will also encourage REJIS to establish and adopt updated incident response procedures that include appropriate incident response training, monitoring and overall accountability.

- 7. The director of general services should encourage REJIS to establish a disaster recovery site that is geographically removed from its data center.**

Agree. General Services will urge REJIS to establish and maintain a disaster recovery site geographically distant from the primary site.

- 8. The director of general services should include criteria in information technology service provider contracts to ensure the confidentiality, integrity, and availability of city information is protected.**

Agree. General Services (through its Information Technology and Procurement Services divisions) will collaborate with the Law Department to establish appropriate language for such contracts by mid-2014.

cc: Mary J. Miller, Chief Information Officer, Information Technology
Cedric Rowan, Procurement Services Manager
Troy M. Schulte, City Manager