



# Audit Department

500 S Grand Central Pkwy Ste 5006 • PO Box 551120 • Las Vegas NV 89155-1120  
(702) 455-3269 • Fax (702) 455-3893

Angela M. Darragh, CPA, CFE, CISA, Director

March 27, 2015

Mr. Don Burnette  
Clark County Manager  
500 South Grand Central Parkway, 6th Floor  
Las Vegas, Nevada 89106

Dear Mr. Burnette:

We recently completed an audit of the Juvenile Justice Services (JJS) FamilyTracs application. The audit was conducted in accordance with our annual audit plan and was deemed necessary due to the confidential and sensitive information that resides on FamilyTracs. It covered JJS cases between July 1, 2013 and December 31, 2013. The last day of fieldwork was July 2, 2014. The objective of this audit was to determine whether the integrity, confidentiality and availability of information within FamilyTracs is maintained.

We identified several system control issues which could affect the confidentiality, integrity, or availability of FamilyTracs data. Specifically, we found that FamilyTracs user account and access administration needs improvement. We also noted that photographs and fingerprints are not consistently taken in accordance with NRS requirements, and records are not always sealed per state statute. We found that FamilyTracs reports and distribution lists need to be reviewed and updated. In addition, we noted that JJS does not have a business continuity plan, a disaster recovery plan, or a FamilyTracs password policy.

A draft report was provided to the Director of Juvenile Justice Services for comment, and his response is included.

We appreciate the cooperation and assistance provided by the staff of Juvenile Justice Services.

Sincerely,

A handwritten signature in blue ink that reads "Angela M. Darragh".

Angela M. Darragh, CPA  
Audit Director



AUDIT DEPARTMENT

# Audit Report



## Juvenile Justice FamilyTracs

March 2015

Angela M. Darragh, CPA, CISA, CFE  
Audit Director

**AUDIT COMMITTEE:**

*Commissioner Steve Sisolak*

*Commissioner Chris Giunchigliani*

*Commissioner Lawrence Weekly*

**TABLE OF CONTENTS**

**BACKGROUND ..... 1**

**OBJECTIVES, SCOPE, AND METHODOLOGY..... 2**

**RESULTS IN BRIEF ..... 3**

**DETAILED RESULTS ..... 4**

**User Account Administration Needs to be Improved (High Risk) ..... 4**

**DCFS (State) Has More Access than Necessary (High Risk) ..... 6**

**System Security Violation Log Not Reviewed (High Risk)..... 6**

**Fingerprints not Taken During Booking (High Risk) ..... 7**

**Photographs Not Taken or Not Removed from Files (High Risk) ..... 7**

**Personal Property Listing Not Completed During Booking (High Risk) ..... 8**

**Records Not Sealed Timely (High Risk)..... 8**

**FamilyTracs Reports Not Complete or Erroneous (High Risk) ..... 8**

**Out of Date Report Distribution Lists and Network Access (High Risk)..... 9**

**No Business Continuity or Disaster Recovery Plan (High Risk) ..... 10**

**No Password Policy for FamilyTracs (Medium Risk)..... 10**

**No Release Information on Admissions Log (Medium Risk) ..... 10**

**MANAGEMENTS RESPONSE..... 12**

**BACKGROUND** The Department of Juvenile Justice Services (JJS) provides intervention, guidance, and control services for youth ages 18 and under involved in delinquency and truancy. It promotes partnerships between youth, families, the community and Juvenile Justice Services.

The main office for Juvenile Justice Services is located at 601 North Pecos Road, Las Vegas, Nevada 89101. However, the department also has five neighborhood centers located throughout Las Vegas and Henderson, Nevada.

Juvenile Justice Services is primarily governed by Nevada Revised Statute (NRS) 62H. Specifically, NRS 62H.100 covers the guidelines over the sealing and unsealing of juvenile records. Further, NRS 62H.210 governs the collection and storage of information gathered on children by Juvenile Justice Services. The regulation requires that a unique number be assigned to each child in the system for identification purposes. The statute also instructs the department on the type of information required for each child: basic demographic information, the charges for which the child is referred, dates of detention, disposition information and petition filed (as applicable).

NRS 62H.230 requires that probation departments annually analyze and submit information to the Division of Child and Family Services (DCFS) concerning the disparate treatment of children, and NRS 62H.300 covers data concerning juvenile sex offenders.

Juvenile Justice Services records all of its cases through a database called FamilyTracs. FamilyTracs is an acronym for Family Tracking, Reporting and Automated Case Support. It is a comprehensive, family focused case management application designed to collect and store information on juveniles within the juvenile justice system. The application originally went live in 1998 but has been enhanced several times since then. The application is maintained by department personnel along with a Clark County Information Technology (CCIT) representative. Collectively, they are called the Application Research & Technology (ART) team.

Juvenile Justice Services provides an array of services including:

- Clinical Services – Assessments and treatment services relating to mental health, substance abuse and crisis intervention are offered through the Clinical Services Division.
- Detention – Juvenile Detention Services provide a temporary, secure, holding facility for juveniles ages 8 to 18 that are subject to the jurisdiction of the Court. The facility

has a maximum bed capacity of 192.

- JDAI – Juvenile Detention Alternative Initiatives – this program was launched to help eliminate the inappropriate use of juvenile detention through the development of community-based alternatives through collaborative efforts by a broad group of community stakeholders.
- Juvenile Fines/Fees – The Payment Center located at 601 N. Pecos processes fines, fees, restitutions and reimbursements Monday through Friday.
- Juvenile Records – The Juvenile Records Unit is located at 2980 Meade Avenue, Las Vegas, Nevada 89102. Juvenile records and statistical reports are available by this group.
- Juvenile Work Permits – Juveniles between the ages of 14 and 17 must obtain a work permit. Work permits are available at various Juvenile Justice Services locations during weekdays.
- Probation – A court ordered sanction allows youth to remain in the community under the supervision of a Probation Officer assigned by Probation Services.
- Spring Mountain Youth Camp – A juvenile correctional facility located at Angels Peak in Mt. Charleston that holds approximately 100 adjudicated delinquent youth.

Applicable juvenile justice regulations include:

[NRS 62 & 63](#) Nevada Revised Statutes

[CCC 2.05](#) Clark County Code

## **OBJECTIVES, SCOPE, AND METHODOLOGY**

The objectives of this audit are to determine whether the integrity, confidentiality and availability of information within FamilyTracs are maintained.

Our procedures consisted of interviews with management and staff, a review of applicable regulations, observations, walkthroughs, examination of documentation, and performance of detailed tests and analyses. We assessed system user and administrator access control procedures by comparing a FamilyTracs system user report with employee information from SAP (the County's enterprise resource software) to determine whether employees with access were actively employed by the County and whether access was appropriate based on employee responsibilities. We also searched for duplicate and generic user accounts (IDs) and reviewed system password policy parameters. Additionally, we performed general control procedures of the Clark County Operations Center housing system server equipment and change management control procedures of the system changes and upgrades to FamilyTracs.

We also analyzed the system logs for security violations and related resolutions. Furthermore, we reviewed and compared two different FamilyTracs reports for information content consistency.

We judgmentally selected 25 juvenile justice transactions from a FamilyTracs Arrest Report and traced those records to individual case files within the FamilyTracs application. We reviewed case file information in the Booking, Detention, and Probation departments (as applicable). From a FamilyTracs Sealed Record Report, we judgmentally selected 12 sealed records and five seal exception records for testing. We traced each of the records to its respective case file in FamilyTracs. We also recalculated seal dates based on juvenile birthdays and obtained document support for any records with a delayed seal date.

Our scope included transactions processed between July 1, 2013 and December 31, 2013. The last day of fieldwork was July 2, 2014. 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.

**RESULTS IN BRIEF** There are several FamilyTracs system control issues which could affect the confidentiality, integrity, or availability of FamilyTracs data. Specifically, we found the following:

- User password information is not periodically changed as required by the Clark County Information Technology (CCIT) Security Policy.
- User account administration needs to be improved.
- There is no continuity plan or disaster recovery plan should the FamilyTracs system become inoperative.
- The State has an active IP address exception through the firewall and excessive access to confidential information.
- System logs are not monitored and alerts are not generated or investigated.
- Reports are sent to email accounts of terminated employees.
- Records are not sealed in accordance with NRS requirements.
- Photographs and fingerprints are not taken in accordance with NRS requirements.
- Reports may not be accurate.

We also found individuals with the same title having different access in the following categories (FamilyTracs functional areas): update medical, sensitive, update, update DA, update psychology, update placement, update child haven visitation, system administration, update organization, reset password access, maintenance window, court release, merge, management reports, seal records, management report delete, quash warrants, seal override, SMYC payroll, mug shots, and update court.

## DETAILED RESULTS

### User Account Administration Needs to be Improved (High Risk)

During our review, we found several issues with active users in the three separate applications and related databases for FamilyTracs. Access to the front-end application requires a user account in both the front-end and the database. Withdrawn, No Database Account, and No Front-End-User Account, and Employee Transfers should be disabled immediately as they should not have active accounts in either the front-end application or the database. Generic accounts must be approved by the department head and Clark County Chief Information Officer in accordance with CCIT policy.

The following tables illustrate the exceptions identified in each area:

	Production – Front End	Production – Database
Active	697	3,912
Withdrawn	6	
Generic	2	
No Database Account	49	
No Front End Account		3,264

	Quality Assurance – Front End	Quality Assurance - Database
Active	7	39
Withdrawn	1	2
Employee Transfers		1
Generic		18
No Front-End Account		14

	Development – Front End	Development – Database
Active	1173	24
Withdrawn	202	1
Generic		11
First and Last Names No Match to SAP	686	

In further reviewing access to the FamilyTracs production environment, we found:

- One information technology (IT) employee, two ART team members, and an Accountant with the ability to update/seal records within FamilyTracs, although these functions are not necessary for their normal job duties.
- Individuals with the same job title with different access.
- Five users with no current information technology or database administration affiliation, but had direct access to the database using their production user accounts and passwords.

User account administration needs to be improved to ensure that only valid employees have access to functions and data necessary based on their job duties to protect the confidentiality and integrity of the data.

#### *Recommendations*

1. Disable all accounts for terminated employees.
2. Develop and implement periodic procedures to review FamilyTracs application and database user accounts for appropriate name, status, and access.
3. Implement standard account security features, such as locking out user accounts when there is no user activity over a certain period in accordance with Clark County IT Technology Directive #1 Section IV.C.1.b.
4. Remove access to update and seal records from IT, ART, and accounting employees.
5. Remove database administration access for those users with no IT or database administration job duties.
6. Delete generic accounts or obtain Department Head and CIO approval if they are necessary.

**DCFS (State) Has More  
Access than Necessary  
(High Risk)**

According to NRS62H.210-230, DJJS is required to send the Nevada Department of Child & Family Services (DCFS) juvenile information on children referred to DCFS. The information is encrypted when sent to protect juvenile information. DCFS unencrypts the information for reviewing, monitoring and reporting purposes. It also sends the information to the federal government for tracking and reporting.

The State has an active internal firewall exception for an IP address. The State user account is allowed access through the Quality Assurance environment in a way that may allow them to draw information from any FamilyTracs environment, including production. This access also allows access to confidential information, including the ability to add, modify, and delete data. We believe that this access is excessive. We reviewed the last login for the State user account and noted that the last login was in 2002. Access with the IP address exception could occur with any valid user account and password within the FamilyTracs environment and not necessarily the State user account.

*Recommendation*

1. Review the States access to FamilyTracs and amend such access based on business necessity.

**System Security Violation  
Log Not Reviewed (High  
Risk)**

A system security violation(s) log is typically maintained and monitored for system log on and off activity. Any unauthorized log on attempt or related violation is recorded on this system log with alerts sent to IT personnel to investigate and resolve. Resolutions should also be recorded on the log to verify the handling and closing of violations.

We obtained a sample system log for FamilyTracs which included all other applications on the Oracle platform. The log was voluminous and in its present format was not readily reviewable. The log does not appear to record violations. Also, this log is not monitored and only kept for a limited amount of time. In addition, the log does not create or send alerts to IT personnel when violations occur. This is important, as unauthorized access of FamilyTracs may be accomplished and go undetected.

*Recommendations*

1. Coordinate with Information Technology (IT) to generate a FamilyTracs system log on SSIM.
2. Create procedures to investigate and resolve any alerts generated by SSIM.

**Fingerprints not Taken  
During Booking (High Risk)**

NRS 62H.010(1) states that fingerprints must be taken if a child commits: a felony, gross misdemeanor, sexual offense, or unlawful act using threat, violence or a deadly weapon. Also, NRS 62H.010(3) requires that fingerprints taken for adjudicated juveniles committing a felony or sexual offense must be submitted to the state Central Repository. In addition, DJJS's booking policy states that fingerprints are to be "printed locally and placed in the supervisory box".

We found 118 of 3,023 records reviewed were missing fingerprints in the file. Missing fingerprints could lead to incorrectly identified juveniles.

*Recommendations*

1. Train employees on the procedures for obtaining fingerprints during the booking process.
2. Create, run, and monitor reports to ensure booking procedures are consistently followed.
3. Periodically spot check records to ensure that hard copies of fingerprints are being filed appropriately.
4. Create and implement procedures of verifying on FamilyTracs that fingerprints were obtained before transferring a juvenile to the Detention Facility.

**Photographs Not Taken or  
Not Removed from Files  
(High Risk)**

NRS 62H.010(4) instructs that a child must be photographed for the purpose of identification. It further requires that photographs be destroyed when juvenile court determines that a child is not deemed delinquent. In addition, DJJS's booking policy states that photographs are to be destroyed when no longer needed.

In reviewing FamilyTracs reports covering the audit period, we found photographs were not taken of children brought into juvenile detention in 1,827 of 3,038 arrests. We also found three files where a juvenile's picture was not destroyed when there was no adjudication or case pending. Photographs are necessary for proper identification, but should be destroyed in accordance with NRS.

*Recommendations*

1. Train employees on the procedures for obtaining photographs during the booking process.
2. Create, run, and monitor reports to ensure photographing procedures are consistently followed.
3. Periodically spot check records to ensure that photographs are being destroyed when they are no longer needed.
4. Create and implement procedures of verifying on FamilyTracs that photographs were obtained before transferring a juvenile to the Detention Facility.

**Personal Property Listing  
Not Completed During  
Booking (High Risk)**

The Booking Department should be preparing a personal property listing for all juveniles that are booked and detained for more than a day. In reviewing 25 juvenile case files, we found two instances where the juvenile was detained for several days and a personal property listing was not completed. Adherence to this policy is important to provide facility accountability for detainee possessions.

*Recommendation*

1. Train employees on properly completing the personal property form during booking.

**Records Not Sealed Timely  
(High Risk)**

NRS 62H.100-170 summarizes the guidelines for the sealing and unsealing of juvenile records. Specifically, NRS 62H.140 states that juvenile records are to be automatically sealed when a child reaches 21 years of age. However, NRS 62H.150 addresses limitations on the auto-seal process which states that “if a child is adjudicated for an unlawful act to include: sexual assault, battery with intent to commit sexual assault, lewdness with a child, and a felony involving the use or threat of force or violence, the child’s records must not be sealed before the child reaches 30 years of age”.

In reviewing 12 sealed cases, we found the following:

- Two records which did not have supporting documentation explaining a delay in the sealing process.
- Four records where there was a delay ranging from two and 20 months between a juvenile’s probation expiration date and the court ordered probation termination date.
- Ten records where there was a delay ranging from three to six months between the court termination date and a juvenile’s record being sealed.

Existing JJS “records sealing” procedures are not adequately ensuring the consistent, timely sealing of cases. With these delays, sensitive and confidential juvenile records are being held open longer than statutes require, and are therefore susceptible to unauthorized view and/or use.

*Recommendation*

1. Revise existing procedures to ensure records are sealed in accordance with NRS requirements.

**FamilyTracs Reports Not  
Complete or Erroneous  
(High Risk)**

To obtain all the information (fields) needed for testing transactions, we had to merge two different FamilyTracs reports (booking and arrest). In combining the two reports and reviewing the output, we found 30 (arrest) transactions that were only listed

in the arrest report, and another 15 transactions that were only listed in the booking report.

Also, we selected 25 juvenile justice transactions from this merged report for further testing. In tracing these transactions to the individual files found in FamilyTracs, we found in 8 of the 25 records where the household information was different than the information in the report. We also noted in 11 of the 25 records that a picture existed in the individual's file, whereas the report indicated that no picture had been taken of the juvenile.

Information between FamilyTracs reports should be consistent, and information in the reports should agree to individual case information found directly on the system. DJJS's written policies do not include procedures for verifying outputs (reports) prior to being distributed, so discrepancies such as those identified during our testing may not be identified. These issues indicate concerns with the reliability of information in reports used by DJJS.

#### *Recommendation*

1. Create and implement a written policy of periodically reviewing FamilyTracs reports (and report parameters) to ensure appropriate information is being captured.

#### **Out of Date Report Distribution Lists and Network Access (High Risk)**

We obtained and reviewed a list of DJJS reports and related distribution lists. We found in reviewing the distributions list that two of the employees receiving reports are no longer County employees. In these cases, the employees have active email addresses, but they have not been accessed since the employment terminated. We also found two State employees who we were not able to verify as current employees.

Typically, a distribution listing for reports containing confidential information should be monitored closely and updated timely to ensure that only appropriate personnel are receiving and have access to the sensitive information.

During our testing, we also found that numerous reports with confidential information are stored on network folders accessible by many employees in various departments and by outside entities (including LVMPD and NLVPD). We found that of five groups with access to reports, seven active users are former employees and five other users had either transferred or were rehired to another department and should not have access. Five vendors have access and should be verified as needing continued access. These issues are significant as they affect the confidentiality of sensitive juvenile information.

#### *Recommendations*

1. Develop and implement periodic procedures to review distribution lists of and direct access to folders containing DJJS FamilyTracs reports.
2. Implement procedures to disable email accounts for terminated employees.

#### **No Business Continuity or Disaster Recovery Plan (High Risk)**

Every department should have written business continuity and disaster recovery plans. The business continuity plan should consist of alternative processes, procedures and location(s) to consider should existing business resources become unavailable. The disaster recovery plan should include business processes and procedures to regain or restore existing operational resources and to ensure that existing and historical information is retrievable or recoverable should a disaster occur. Implementing such plans is necessary to prevent disruptions to operations and ensure that sensitive information is safeguarded and accessible.

We found there is no business continuity plan or disaster recovery plan in place for DJJS and the FamilyTracs application.

#### *Recommendation*

1. Work with CCIT to produce written business continuity and disaster recovery plans.

#### **No Password Policy for FamilyTracs (Medium Risk)**

There is no password policy in effect for the FamilyTracs system. According to Clark County Information Technology Security Policy (CCIT Security Policy) (C) System Access Control/(2)(a)(1) Authentication, user passwords must be at least eight characters in length and consist of two or more of the following: capital letters, lower case letters, numbers, and special characters (%\*\$@!). User passwords should not include common names or phrases. User passwords must be changed every 90 days and may not be reused for at least six password change periods.

Implementing password requirements is important to ensure user accounts are not easily compromised, which affects the confidentiality and integrity of the data.

#### *Recommendation*

1. Coordinate with CCIT on implementing a user password policy for the FamilyTracs system.

#### **No Release Information on Admissions Log (Medium Risk)**

Information on juveniles being released from the Clark County Juvenile Detention Facility is required to be entered onto the Admissions Log. As such, release information between FamilyTracs and the Admissions Log should be consistent. However, we found

in four of the 21 records reviewed (where a juvenile was detained) where the release information was not entered onto the Admissions log on the date a juvenile was released. We also found one record where the release date in the Admissions log was different than the release date in FamilyTracs.

*Recommendations*

1. Monitor adherence with the procedure for entering release information on the Admissions log and provide additional training as necessary, or
2. Eliminate this manual process and rely on release information entered on FamilyTracs.



**Department of Juvenile Justice Services  
Director's Office**

601 N Pecos Rd • Las Vegas NV 89101-2408  
(702) 455-5210 • Fax (702) 455-5216

**John M. Martin, Director**  
Patrick Schreiber, Assistant Director



March 27, 2015

Clark County Audit Department  
Attn: Angela Darragh, Director

The Clark County Department of Juvenile Justice Services agrees with the audit results and have initiated the actions identified in the MS Excel workbook entitled [A1.8 Audit Report Action Plan Form for Audit Committee.xlsx](#) in order to improve upon the business practices identified by the audit report that are within the control of the Department. Some of the specific recommendations made by the audit report have already been implemented. We are committed to not only make corrections in the areas of concern, but also to implement business practice changes to ensure that these defects do not reoccur in the future.

We have further started dialogue with Information Technology (IT) to address those areas of concern that are within their purview, and are understanding that some of the issues identified by audit already have remedies in development due to County-wide impact. We are also exploring the replacement of our data management system due to the high costs involved in making necessary improvements to the software in its current platform.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "J.M. Martin".

John M. Martin, Director  
Clark County Department of Juvenile Justice Services