CR NEWS

HIGHLIGHTS:

CHILD SAFETY ALERT LIST

The Child Safety Alert File was created to help the Department of Family and Protective Services (DFPS) locate a family for purposes of investigating a report of child abuse or neglect in accordance with Texas Family Code Sec. 261.3022. If DFPS is unable to locate a family for purposes of investigating a report of child abuse or neglect, DFPS may seek assistance from the appropriate county attorney, district attorney, or criminal district attorney with responsibility for representing DFPS as provided by Section 264.009.

If it becomes necessary for DFPS to request assistance, the county attorney, district attorney, or criminal district attorney, as applicable, may file an application with the court requesting the issuance of an ex parte order requiring the local police department or sheriff's office to place the alleged offender and victim into the Texas Crime Information Center's (TCIC) Child Safety Check Alert List. The application for the issuance of an ex parte order must include a summary of the report of child abuse or neglect the DFPS is attempting to investigate and the efforts DFPS has taken to locate the family. If the court determines, after a hearing, that DFPS has exhausted all means available to the department for locating the family, the court shall approve the application and order DFPS to notify the local law enforcement agency to place the family on the Child Safety Check Alert List.

Once an applicable ex parte order has been issued and received by the law enforcement agency, the record must be entered into TCIC.
The following information should be included in your entry:

- The name, sex, race, and date of birth (or approximate date of birth) of the family member alleged to have neglected or abused the child
- The name, sex, race, and date of birth (or approximate date of birth) of the child who is subject of the report
- The type of alleged abuse or neglect against the child
- The family's last known address
- Note if the actual date of birth is unknown, the month and day can be entered as 0000 but a valid year must be used.

Law enforcement agencies are to pack the Child Safety Check Alert List record with all information known to be true and valid, even if that information is not provided by DFPS on the data entry form. If known, personal descriptors and vehicle information can be included in the record in addition to driver's license (OLN) information, scars marks and tattoos (SMTs) and any caution or medical conditions (CMC) of either the primary child or alleged offender. For both the child and alleged offender, additional information such as alias names, dates of birth, scars, marks and tattoos as well as vehicle information can be entered by using transaction code ESLS. Similarly, this data can be removed from the record using the transaction code XSLS.

When a law enforcement officer provides DFPS the current residential address of a child or children listed in the TCIC Child Safety Check Alert List, the entering agency must clear the record using the clear transaction (CSL). A cancel transaction (XSL) is used when it is determined the record is invalid; for example, the court order which was the basis for the record has been revoked.

RAPID DNA or RAPID DNA ANALYSIS (FAQs)

Q: What is Rapid DNA or Rapid DNA Analysis?

A: Rapid DNA, or Rapid DNA Analysis, describes the fully automated (hands free) process of developing a CODIS Core STR profile from a reference sample buccal swab. The "swab in – profile out" process consists of automated extraction, amplification, separation, detection and allele calling without human intervention.

As of March 2014, no Rapid DNA instruments have been approved by the FBI that meet this definition.

Q: What is the Rapid DNA Index System (RDIS)?

A: Rapid DNA Index System (RDIS) is the proposed fourth tier of NDIS; a fully integrated system capable of performing reference sample buccal swab STR analysis in 1-2 hours and initiating DNA enrollment and searches from a police booking station.

Q: How is the FBI involved in the development of Rapid DNA technology?

A: The FBI established a Rapid DNA Program Office in 2010 to direct the development and integration of Rapid DNA technology for use by law enforcement. The Program Office works with the Department of Defense, the Department of Homeland Security, the National Institute of Standards and Technology, the National Institute of Justice, and other federal agencies to ensure the coordinated development of this new technology among federal agencies. The Program Office also works with state and local law enforcement agencies and state bureaus of identification through the FBI's Criminal Justice Information Services Division Advisory Policy Board to facilitate the effective and efficient integration of Rapid DNA in the police booking environment.

Q: What is the goal of the FBI's initiative on Rapid DNA development?

A: The goal of the FBI's Rapid DNA initiative is to develop commercial instruments capable of producing a CODIS-compatible DNA profile within two hours and to integrate those instruments effectively within the existing CODIS structure to search unsolved crimes while an arrestee is in police custody during the booking process. The FBI has been working on how to integrate this technology first into CODIS laboratory operations and then into police booking locations.

Q: Do these goals include the use of Rapid DNA technology on crime scene (forensic) samples?

A: At this time, these goals do not include the use of Rapid DNA technology on crime scene (forensic) samples because of the differences between forensic and known reference (offender/arrestee) samples. These differences may include the nature or type of sample, typical sample quantity and potential for reanalysis. A forensic sample may not be amenable to fully automated processing due to limitations in its quality and quantity.

Q: Is the Rapid DNA technology currently operational?

A: Several manufacturers have developed prototype instruments for Rapid DNA analysis. These instruments are now being tested and evaluated by the FBI Laboratory and several other Federal agencies, such as the National Institute of Standards and Technology (NIST) and the Army Crime Laboratory. In January 2013, the manufacturers of the prototype instruments attended a Scientific Working Group on DNA Analysis Methods (SWGDAM) meeting to discuss their instruments and obtain feedback on validation. Because developmental validation is a crucial first step in the commercial use of these instruments, SWGDAM, through its Rapid DNA Committee, has established a dialog with the manufacturers to assist them in their validation effort (see SWGDAM FAQs at https://www.swgdam.org/faq). The FBI does not consider these Rapid DNA instruments for Rapid DNA Analysis operational until all applicable QAS validation standards are met and all necessary NDIS approvals are in place.

Q: Can a Rapid DNA instrument be used by an accredited forensic laboratory to develop DNA profiles from known reference samples?

A: If the following assumptions are met and a laboratory is in compliance with the FBI Director's Quality Assurance Standards (QAS) enumerated below, a Rapid DNA instrument may be used to develop DNA profiles from known reference samples. As of March 2014, use of a Rapid DNA instrument by an accredited laboratory would be limited to Modified Rapid DNA Analysis defined below.

Assumptions:

1. A Rapid DNA instrument must be operated by an accredited forensic laboratory as required by the DNA Identification Act of 1994;

2. An accredited forensic laboratory must develop a DNA profile from a known reference sample; and

3. The Rapid DNA instrument must be used to conduct Modified Rapid DNA Analysis. **Modified Rapid DNA Analysis** describes the automated (hands free) process of developing a CODIS Core STR profile from a known reference sample. This process consists of integrated extraction, amplification, separation, and detection without human intervention, but requires human interpretation and technical review.

Use of a Rapid DNA instrument to conduct Modified Rapid DNA Analysis on known reference samples by an accredited laboratory requires compliance with the following:

- Documentation of the developmental validation for the Rapid DNA instrument in accordance with the FBI Director's QAS for DNA Databasing Laboratories (Standard 8.2);

- Documentation of internal validation of the Rapid DNA instrument by the accredited laboratory in accordance with QAS standard 8.3;

- Use of an NDIS approved DNA STR typing test kit (DNA typing kit with corresponding part number or catalogue number). A Modified Rapid DNA analysis incorporating an NDIS approved DNA typing kit is permitted as long as there is documentation that the chemistries and concentrations are exactly the same as the NDIS approved DNA STR typing kit (see the CODIS and NDIS Fact sheet for list of NDIS approved DNA STR typing kits)

- Manual interpretation and review of the data by a qualified DNA analyst (as required by QAS Standards 9 and 12); or use of an NDIS approved Expert System in accordance with the NDIS Operational Procedures and QAS; and

- Compliance with all QAS, including but not limited to, the use of controls.

If all of the above conditions are met, an NDIS participating laboratory is permitted to upload authorized known reference DNA records developed using a Modified Rapid DNA Analysis to CODIS.

In order for an accredited laboratory to perform Rapid DNA Analysis (unmodified) of known reference samples for upload to CODIS, both the DNA STR typing test kit and Expert System must be approved by NDIS in accordance with the NDIS Operational Procedures and QAS.

Q: Can a Rapid DNA instrument be used by an accredited forensic laboratory to develop DNA profiles from crime scene (forensic) samples?
A: No, the analysis of crime scene (forensic) samples by an Rapid DNA instrument would not be compliant with the FBI Director's Quality Assurance Standards for Forensic DNA Testing Laboratories (Forensic QAS Standards 9.4 and 12.2). The FBI and SWGDAM are not currently considering or discussing the application of the QAS to the analysis of crime scene (forensic) samples by a Rapid DNA instrument. Forensic DNA records that are not compliant with the FBI's QAS are not permitted to be searched in or uploaded to CODIS.

Q: When will law enforcement agencies be able to use Rapid DNA?
A: While the manufacturers are working on validation of these instruments, the FBI has been identifying and working on resolving issues that will need to be addressed to achieve the goal of using these Rapid DNA instruments in the booking environment. For example, the DNA Identification Act of 1994 (42 U.S.C. §14132) requires that the DNA records be generated by accredited laboratories in compliance with the FBI Director's Quality Assurance Standards (QAS). Thus, legislation will be needed in order for DNA records that are generated by Rapid DNA instruments outside an accredited laboratory to be uploaded to the National DNA Index System (NDIS). Additionally, issues relating to the validation and certification of the Rapid DNA analysis instruments must be resolved before implementing this new technology as part of the booking process. The FBI recognizes that issues relating to NDIS approval/certification of the instruments and training of law enforcement personnel using the approved instruments must be resolved so that this new technology is used in a manner that maintains the quality and integrity of CODIS and NDIS.

Q: Is there an expected implementation date for the Rapid DNA technology?
A: As a consequence of these outstanding issues and the need for legislative changes, it is difficult to estimate when law enforcement agencies will be able to search profiles developed by a Rapid DNA instrument in CODIS. SWGDAM will continue its priority efforts for developing recommendations for revisions to the FBI Director's QAS. The FBI will continue its collaboration with other Federal agencies in the testing and evaluation of the available Rapid DNA instruments as well as support for legislative changes necessary for implementation of this technology.

You may wish to check these FAQs periodically for progress updates on Rapid DNA as the FBI works to establish the proper foundation for the use of this technology through validation, guidelines, training, etc.

WINDOWS XP COMPENSATORY MEASURES

As you are probably aware, Microsoft has indicated that it will discontinue support for the Windows XP operating system on April 8, 2014. After this date, Microsoft will no longer provide free security updates or technical support for Windows XP. Security updates patch vulnerabilities that may be exploited by malware and help keep users and their data safe. PCs running Windows XP after April 8, 2014, should not be considered to be protected, and additionally, will not be considered to be compliant with the FBI's CJIS Security Policy. If you are unable to remediate any XP based PCs that connect to DPS by April 8, DPS suggests that you employ the following compensatory measures

(The following information has been derived from the United States Computer Emergency Readiness Team. For additional information, please reference http://www.us-cert.gov/ncas/alerts/TA14-069A-0)

General Compensatory Measures for Windows XP (XP) Systems

• For those that are unsure what OS they may be running, Microsoft provides an, "Am I running XP?" site (http://goo.gl/PFbCpg). Upon visiting the site, a large message displays to indicate whether the end user is or is not running XP.

• Microsoft is encouraging users to upgrade to Windows 7/8, but reminding them that older computers may not meet system requirements. In these cases, Microsoft suggests upgrading to a new computer. For those looking to upgrade to a new computer, Microsoft is also offering Laplink PC mover Express to offer free assistance in moving data from an old XP computer to a new Windows PC.

• Microsoft will continue to support the Microsoft Security Essentials product through July 14, 2015. For enterprise customers this includes System Center Endpoint Protection, Forefront Client Security, Forefront Endpoint Protection and Windows Intune.

• Microsoft will also offer *Custom Support* Agreements as a last resort for those that do not expect to complete migration to a new OS in time. Use of this support requires additional funds to be expended on a per computer basis.

• Of 26 antivirus vendors, AV-TEST (http://goo.gl/PCLZNL) provides a list of 22 that will continue to push updates to their suites on XP, which will aid in protection after Microsoft ends support.

Supplementing Security: Custom Built Applications

Many organizations may find upgrading to a different OS challenging as some have chosen to build custom applications on XP. Of these custom-built applications, some are still in use for mission-critical projects today and will not easily transfer to Windows 7/8. The following options, or a combination of them, may be useful for organizations running custom XP applications:

1. Hire the person who built the application to rewrite the application and make it compatible with other operating systems.

2. Shim the app, or "trick" the application into thinking it is running in an XP environment. This option is unstable, risky, and it may not work.

3. Virtualize the application so that it will work in a different operating system.

4. Continue to use the XP computer on an interim basis; however, lock-down administrative rights and do not let anything new be installed on it (virtual applications would be a good route here, as they do not require installations to run). This is a worst-case scenario and would only be a temporary option.

Supplementing Security: Individual End Users

The following recommendations are for individual end users using XP computers until they are migrated to Windows 7/8:

• Air-gap or isolate on separate networks XP computers in order to protect updated machines from being attacked by compromised XP computers.

• Install the final XP update so computers start their unsupported lives protected from the latest known vulnerabilities.

• Install an alternative browser (i.e. Firefox or Chrome) and make it the default. XP comes with Internet Explorer but it only supports up to IE 9, making the security features of IE 10 and 11 unavailable.

• Fully patch Microsoft Office to reduce the chances of it being used to compromise the XP computer.

• Uninstall unused third-party software. The older it is, the more likely it is to be vulnerable.

• Consider disabling or uninstalling browser plugins for third-party software, and set the browser to ask what to do with PDFs, etc., rather than opening them by default.

• Install up-to-date firewalls and anti-virus software.

• Keep the computer on a trusted network behind a NAT router, which acts as a hardware firewall.

• Upgrade to Windows 7/8 as soon as possible.

NATIONAL SEX OFFENDER

At its December 2006 and June 2009 meetings, the CJIS Advisory Policy Board (APB) approved renaming the NCIC Convicted Sexual Offender Registry File to the National Sex Offender Registry (NSOR). In addition, the CJIS APB approved changes to the following:

- criteria for entry,
- FBI Number Field,
- Sex Offender Registry Notices,
- $.Q notifications,
- clear and audit procedures,
- validation requirements,
- record retention;
- identified essential data elements; and
- added new base and supplemental data fields.

Although the file is being renamed NSOR, the MKE translation will not be changed from SEXUAL OFFENDER.

DPS will be implementing these changes April 13, 2014.

Due to the large quantity of changes to the Convicted Sexual Offender Registry File, the chapter has been reissued. Refer to the NCIC 2000 Operating Manual to view the National Sex Offender Registry file in its entirety.

NCIC TOUs, as well as, the NCIC Operating and Code Manuals are posted in their entirety on the TCIC2000 website:

http://www.dps.texas.gov/tcic2000project/TOU/index.htm

MONTHLY VALIDATIONS

On a monthly basis, the NCIC 2000 System extracts active records on file for validation purposes.

Validation obliges the ORI to confirm that the record is complete, accurate, and still outstanding or active. Validation is accomplished by reviewing the entry and current supporting documents, and by recent consultation with any appropriate complainant, victim, prosecutor, court, nonterminal agency, or other appropriate source or individual. In the event the ORI is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority must make a determination based on the best information and knowledge available whether or not to retain the entry in the file.

A signed certificate is required from every agency that receives one, as this certifies the agency has reviewed all records and taken the appropriate actions, whether that entails updating the information or removing an entry altogether. Please keep the original on file and email to TCIC.Operations@dps.texas.gov or fax a copy to (512) 424-5916 and (512) 424-7164. All originals received will be sent back to the agency.

Also, keep in mind the due date is the deadline for turning in the certificate. If we have not received a certificate by 5pm, the delinquent agency's records are eligible to be purged.

Again, mailing in the original is no longer required. If you have questions regarding the new procedure, contact Anne Kondratick at (512) 424-2898 or Adina DeCuire at (512) 424-5949 with TCIC Operations.

TEXAS ONLY WANTED PERSON

In an effort to increase officer and public safety and to increase visibility to the warrants currently held in the Texas-Only Wanted Person file, the Department has elected to eliminate the Texas-Only Wanted Person file. Also, due to the FBI's modification to the Extradition Limitation Field (EXL) all wanted person records now meet the criteria for entry into NCIC.

On January 1, 2014 entry capability into the Texas-Only Wanted Person files was disabled. Existing Texas-only wanted person records remain on file; however, the entries for any new records are not allowed. During the validation process and as records purge due to their retention schedule, agencies are encouraged to review their Texas-Only entries to examine whether or not they will re-enter the record utilizing the MKE/EW. This will allow agencies to address a smaller number of records over a period of time, rather than handling all of their Texas-Only records in a single instance. Agencies have until January 1, 2016 to address any remaining Texas-Only wanted person records. After this date, the records will be purged from the database.

Disabled message keys: ECW, EE, EE-C, EW-T

ELECTRONIC ARREST REPORTING (EAR)/LIVESCAN

To agencies that are submitting class C arrests, please make sure that you are using the proper class C offense codes with the ADN 233. It is very important that you use the ADN code 233 to close out the arrest. DPS receives a large amount of class C arrests without the ADN 233 and these arrests hit an error report that has to be corrected before the arrests can be applied to CCH.

Livescan DOs and DON'Ts:

DOs

- **Do** check all responses
- **Do** review reject errors, correct, and retransmit
- **Do** submit alias names, example: Slick,XX ("Slick,Nickname" is no longer valid)
- **Do** use current offense codes (version 14)
- **Do** transmit adult class C offenses
- **Do** use corresponding ADN for class C **(233)** and federal **(234)** offenses

DON'Ts

- **Do Not** transmit out of state probation and paroles via livescan
- **Do Not** resubmit for corrections or added charges (mail/fax to DPS or use the CJIS site: https://cch.dps.texas.gov)
- **Do Not** use offense code 99999999
- **Do Not** submit Juvenile class Cs
- **Do Not** populate an arrest record with identification data base on a name search from a DL search

If you have any questions or concerns about electronic arrest reporting, please contact your DPS field representative or the livescan coordinator, loann.garcia@dps.texas.gov or (512) 424-2409.

NO MORE AGENCY ADMINISTRATORS IN TDEx

You may have noticed by now that the Agency Administrator (AA) duties have been removed from all users who held that role. That decision was made on March 28, 2014.

The AA role provided each agency the ability to perform many functions for their personnel. The AA could create accounts for those at their agency who needed to access the Texas Data Exchange (TDEx), they could reset passwords, and they could audit the use of TDEx by those at their agency.

Some time back, one of those duties became obsolete. The decision was made, by the Texas Department of Public Safety, not to add any new users to TDEx as we began our transition to N-DEx. We were encouraging all those who wanted access to the data to obtain Law Enforcement Enterprise Portal (LEEP) accounts. This would allow them to gain N-DEx access.

Though this decision was made, and AAs were asked not to create any new accounts, we noticed that the total number of TDEx accounts continued to grow month after month. Because we were unable to determine which AAs were still creating accounts, we decided it would be best to remove the AA role from all users. This was the only way to ensure that no new accounts would be created.

This means that the other functions of the AAs are no longer available either. Therefore, should any user need to have their password reset, they will need to contact the TDEx office at 512-424-2629 or tdex@dps.texas.gov

We apologize for any inconvenience this may cause, but we felt it was the only option we had.

For information on getting a LEEP account, please feel free to contact our office at the phone number or e-mail above.

N-DEx Success Story of the Year Award
2014

Have you had success using N-DEx?

Submit your story and enter N-DEx's new Success Story of the Year Award program.

As the national leader in enhancing public safety and reducing crime through effective information sharing, the FBI's National Data Exchange (N-DEx) has helped local, state, tribal, and federal agencies across the nation generate case leads, protect victims, and solve crimes.

In an effort to identify and highlight these efforts, N-DEx has implemented a *Success Story of the Year Award* that showcases a situation in which N-DEx information made a significant contribution to an investigative, prosecutorial, or preventive action that has taken place in the last two years.

If you are an officer, investigator, or analyst who uses N-DEx and has a story to share for consideration, please contact the N-DEx Program Office via e-mail at **ndex@leo.gov**.

The submission deadline for this year's award is **August 1, 2014**.

For more information about N-DEx:
ndex@leo.gov
304-625-4357

CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS)
&
JUVENILE JUSTICE INFORMATION SYSTEM (JJIIS)
REPORTING CODE CHANGES

Effective September 1, 2014, Criminal Justice Information System (CJIS) and Juvenile Justice Information System (JJIS), reporting codes will have an impact on a county's Open Offense Report and the County Combined Completeness Percentage Report. The Open Offense Report provides the open offenses for a specified date range and the County Combined Completeness Percentage Report provides a five Year County combined completeness percentages. These changes will have an effect on the next five (5) year window for 2015, for years 2009-2013. This will impact the status of some reporting codes changing from closed to open. If a reporting code changes an offense to open status, DPS will display the offense on the Open Offense Report. Open offenses will cause a decrease in the County Combined Completeness Percentage Report. Please keep in mind, the five year County Combined Completeness Percentage Report is used by various state agencies to assist with determining Grant Funding eligibility for Criminal Justice and Non-Criminal Justice grantees within each county.

Example:

Juvenile Code: 612, the case has been referred to the prosecutor, will no longer be closed and will require additional reporting.

To assist counties with this change, the CJIS Support Unit Field Representatives will be working with agencies throughout 2014. The field representatives will be able to explain the changes, explain how and when to report the final dispositions and assist with Open Offense Reports. These reports are available to authorized CJIS Site users. To become an authorized user, you may request access at https://cch.dps.texas.gov Click on request access.

CJIS FIELD SUPPORT CONFERENCE

The CJIS Field Support Conference will be held for three days during the week of 11/17/2014-11/21/2014 at the Galveston Island Convention Center. As soon as the details have been finalized, an announcement will be made on the listserv that will include a link to the Online Registration. We look forward to seeing you in November!

If you have not already done so and would like to subscribe to the listserv, please follow these steps:

1) Send an email to LISTSERV@LISTSERV.DPS.TEXAS.GOV. Make sure that:

   a. The subject line is left blank.
   b. The message body is clear/blank (including signatures).
   c. Type: SUBSCRIBE CJISJJIS FirstName LastName, in the message body.

2) Once you have completed that, you will receive an email stating that "You are now subscribed to the CJISJJIS list."

LATENT SITES

As administrator of the State AFIS (Automated Fingerprint Identification System), the Department of Public Safety works to maintain the reliability of the system, and makes every effort to keep it at optimal performance levels. But we can't do this alone. Everyone must do their part to protect the integrity of the system, and work to minimize backlogs that can cause system issues.

One of the biggest issues plaguing the system today, is the backlog of TL/I's (Ten-print to Latent Inquiries) waiting to be verified. Failure to maintain the TL/I verifications causes the number of transactions waiting to be verified to grow, which in turn, causes issues and "bogs down" the main AFIS system. This directly affects the DPS Central Site and the remote site locations for both 10-print and latent processing. While we realize that the number of TL/I's has increased due to the processing of fingerprint submissions now being accepted from the Driver's License Offices, it is imperative that these be worked. DPS is monitoring the TL/I backlog, and notifying agencies that maintain a large backlog of un-worked TL/I's. However, if an agency cannot keep up with their TL/I traffic, DPS may be forced to purge the latent images stored by that agency to maintain the overall wellbeing of the system. When an operator leaves due to retirement, promotion, etc., it is essential for you to notify DPS right away so that the operator's log-in can be removed, and the TL/I's forwarded to another operator who can verify them, and keep them from continuing to build up.

In addition to trying to minimize backlogs of transactions in the system, we must all work to make sure that only qualified individuals have access to the AFIS system. When it comes to protecting the integrity of the system, we all realize the value and importance of having trained and qualified personnel. DPS has policies and procedures in place, which are spelled out in the Texas DPS Latent Workstation User Agreement, to try to make sure that only authorized individuals are using the system. It is a violation of the user agreement, and the CJIS Security Policy, for unauthorized latent print technicians, who have not been trained or tested by the DPS Crime Lab, to log onto a remote site AFIS workstation by utilizing the login credentials of another authorized user. Allowing such behavior can result in the suspension of service and possible removal of equipment (for sites whose workstation is owned by the Department of Public Safety). Maintaining a staff of qualified individuals can be challenging at times when employees retire or move on in their careers. If you need to schedule training and testing on AFIS for any new employees, please contact Jenny Hall, AFIS Latent Supervisor, at (512) 424-7605, or by email at jenny.hall@dps.texas.gov.

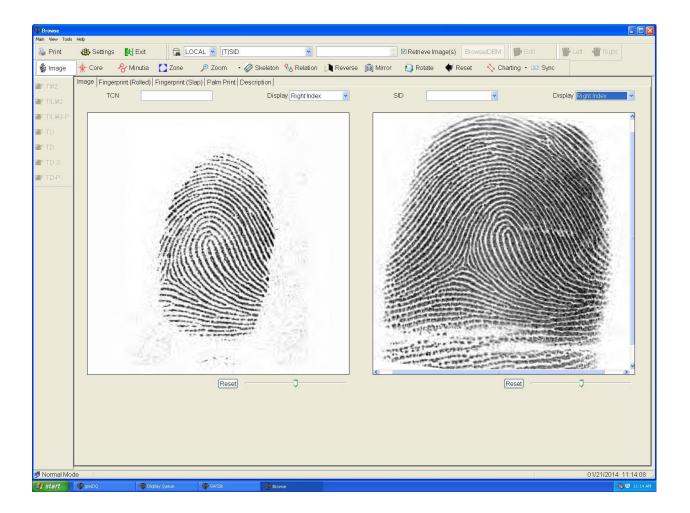Over the years, AFIS has become a vital system that is relied upon by law enforcement agencies and authorized non-criminal justice agencies. It automates the processing of arrest and applicant fingerprint submissions, and provides the ability to search latent fingerprints and palm prints obtained from crime scenes against the fingerprint/palm-print databases of persons previously arrested, or who have been through a fingerprint background check. Additional benefits include:

- Updating Criminal History Records in a timely manner
- Electronically forward submissions to the FBI for processing and updating national databases.
- Electronically updating the local archive system

These functions are extended to local law enforcement agencies by a network of remote input devices placed at various police departments and sheriff's offices throughout the state. With that in mind, we must all work together to keep the system functioning efficiently for everyone.

TEXAS STATE AFIS SYSTEM ACCEPTING DRIVER'S LICENSE PRINTS

On January 1, 2014, driver's licenses offices throughout the state of Texas began taking plain impressions of all ten fingers. The images are being captured in the form of NIST Type 14 "Identification Flats", and are being submitted to the state AFIS system. Once submitted, the prints are searched against the images already existing in the system. If no match is found, the prints are registered in AFIS, thus making them available for latent case work. As the name suggests, the images are from submissions captured from slap impressions of both hands, with the individual fingerprint images being segmented from the plain impressions, as opposed to the traditional fingerprint images which are rolled individually, nail to nail. Because of the nature of the slap impressions (less surface area, core only), it should be easy to differentiate between the prints segmented from a plain impression, and the ones obtained from full rolled impressions.

Given the large population of drivers, or individuals with state issued ID cards, it is anticipated that latent hits will be generated on these prints. In addition, there will also be an increase in the number of TL/I's (ten-print to latent inquiry) generated.

The processing flow for the driver's license prints follows that of an applicant transaction, and only minimal demographic data is being stored in AFIS. The images will be used to assist in identifying an individual. Driving Records will continue to be maintained by the Driver's License Division, and Criminal Records will continue to be maintained by the Law Enforcement Services Division.

The success of this new capture methodology is yet to be determined. Texas Department of Public Safety has asked latent examiners throughout the state, to report hits on these prints, so the success can be monitored. It will take some time to capture the prints for drivers and ID card holders, and get them entered into the system. Many of the DL prints will hit on existing records as many individuals already have prints registered through the applicant background process, or an arrest event. Nonetheless, any increase to the number of records registered in the AFIS system, the better the odds of solving crime.

FINGERPRINT PROCESSING REPORT

January - March, 2014

Criminal Transactions Submitted to AFIS

The following information reflects the total number of criminal tenprint fingerprint transactions submitted to AFIS.

Number of Transactions Submitted Electronicaly	196,726
Number of Transactions Submitted via Hard-Card	18,234
Total number of Criminal Transactions Submitted to AFIS	**214,960**

Applicant Transactions Submitted to AFIS

The following information reflects the number of applicant tenprint fingerprint transactions submitted to AFIS.

Number of Transactions Submitted Electronically	26,567
Number of Transactions Submitted via Hard-Card	13,589
Total number of Applicant Transactions Submitted to AFIS	**40,156**

Fingerprint Supported Dispositions

The following information reflects the number of fingerprint supported dispositions submitted electronically to AFIS.

Total number of Custody Transactions Submitted to AFIS	**235**

Manually Processed Fingerprints

The following information reflects totals for fingerprint transactions that were manually verified or classed and searched.

Criminal Cards (including TDC faxes)	851
Applicant Cards	2,745
Deceased (known and unknown)	395
Total number of Manually Processed Fingerprints	**3,991**

Mobil ID Transactions Processed

The following number reflects the number inquiries processed on the MID System (Mobil ID System)

Total Number of Mobil ID Transactions Processed	**1,712**

AFIS Database Counts

The information below reflects the database counts at the beginning of each month.

	Rolled Print DB	Palm Print DB	Slap Print DB	Latent DB	Latent DB - Palms	Mobil ID DB
January	11,448,469	1,239,855	5,755,586	131,678	21,728	7,541,875
February	11,508,185	1,258,161	5,824,406	131,454	21,973	7,557,484
March	11,566,154	1,277,743	5,892,312	125,594	21,549	7,573,947
April						
May						
June						
July						
August						
September						
October						
November						
December						

DPS IDENTIFICATION SUPPLIES ORDER FORM

TO; CRIME RECORDS SERVICE
TEXAS DEPARTMENT OF PUBLIC SAFETY
PO BOX 4143
AUSTIN TX 78765-4143   Date: _____
FAX: 512-424-5599
Please furnish the following supplies

FORM NUMBER	DESCRIPTION	COUNT PER PKG	QUANTITY ORDERED
CR-6	DPS Applicant Card*	250 p/pkg	
CR-12	DPS Identification Supplies Order Form	100 p/pad	
CR-23	Out of State Probation/Parole Supervision Card	Single cards	
CR-26	Death Notice Form	100 p/pad	
CR-42	Request for Criminal History Check	100 p/pad	
CR-43	Adult Criminal History Reporting Form **with** Preprinted TRN and Fingerprint Card Attached*	100 p/pkg	
CR-43	Adult Criminal History Reporting Form **with** Fingerprint Card Attached*	100 p/pkg	
CR-43J	Juvenile Criminal History Reporting Form **with** Preprinted TRN and Fingerprint Card Attached*	100 p/pkg	
CR-43J	Juvenile Criminal History Reporting Form **with** Fingerprint Card Attached*	100 p/pkg	
CR-43P	Adult Probation Supervision Reporting Form **with** TRN Numbers	200 p/pkg	
CR-43P	Adult Probation Supervision Reporting Form **without** TRN Numbers	200 p/pkg	
CR-44	Adult Supplemental Court Reporting Form	100 p/pkg	
CR-44J	Juvenile Supplemental Reporting Form	100 p/pkg	
CR-44S	Adult Supplemental Court Reporting Form	100 p/pad	
CR-45	Adult DPS Fingerprint Card*	250 p/pkg	
CR-45J	Juvenile DPS Fingerprint Card*	250 p/pkg	
FD-249	FBI Arrest & Institution Fingerprint Card (Felony Card)*	500 p/pkg	
FD-258	FBI Applicant Fingerprint Card*	500 p/pkg	
FD-353	FBI Personal Identification Fingerprint Card*	500 p/pkg	
R-84	FBI Final Disposition Notice	500 p/pkg	
	Fingerprint Card Return Envelopes (For Arresting Agency Only)	100 p/box	

*DPS does not pre-stamp the agency ORI on any fingerprint card. Overnight services are available at ordering agency's expense.

NOTE: Please order minimum of three weeks supply. Please submit order at least 4 weeks prior to depletion of your supplies.

NOTICE: Provide a complete shipping address (PO Box(es) are acceptable).

AGENCY NAME _____

STREEET ADDRESS _____

COUNTY _____ CITY _____STATE TX ZIP _____

ATTENTION _____ PHONE NO. (_____)_____-_____

CRS DIRECTORY

CRS MANAGEMENT

Mike Lesko	Deputy Assistant Director	mike.lesko@dps.texas.gov	512-424-2524
Angie Kendall	Deputy Administrator	angie.kendall@dps.texas.gov	512-424-2471
Michelle Farris	Deputy Administrator	michelle.farris@dps.texas.gov	512-424-7659

ACCESS & DISSEMINATION BUREAU

Don Farris	Manager	donald.farris@dps.texas.gov	512-424-2078
Elaine Smith	Supervisor, Support	elaine.smith@dps.texas.gov	512-424-2023
Sharon Hill	Supervisor, Training & Audit	sharon.hill@dps.texas.gov	512-424-7920
Susie Dial	Supervisor, Training & Audit	susanne.dial@dps.texas.gov	512-424-7927
Darlene Saenz	Supervisor, CHIU	darlene.saenz@dps.texas.gov	512-424-5474
Charlene Cain	CCH Internet Coordinator	charlene.cain@dps.texas.gov	512-424-2090
Jennifer Norton	Budget Analyst	jennifer.norton@dps.texas.gov	512-424-7793
Lisa Garcia	Billing Technician	lisa.garcia@dps.texas.gov	512-424-2912
Assistance Line	Record Checks		512-424-5079
Assistance Line	Secure Site		512-424-2474
Tierra Heine	CJIS/JJIS Forms and Fingerprint Card Supplies	**Fax order form to**	512-424-5599
	Order Forms located at ftp://crspub.dps.texas.gov/		

CRIMINAL HISTORY RECORD INFORMATION PROCESSING BUREAU

Ursula Cook	Manager	ursula.cook@dps.texas.gov	512-424-2407
Cassandra Richey	Supervisor, CJIS Field Reps	cassandra.richey@dps.texas.gov	512-424-2479
Brittany Chromcak	Section Supervisor, Data Integrity	brittany.chromcak@dps.texas.gov	512-424-7290
Nicole Berry-Moss	Dayshift Supervisor	nicole.berry-moss@dps.texas.gov	512-424-2216
Brandy Turner	Dayshift Supervisor	brandy.turner@dps.texas.gov	512-424-7281
Lenore Hemstreet	Evening Supervisor	lenore.hemstreet@dps.texas.gov	512-424-2473
Holly Morris	EDR Coordinator	holly.morris@dps.texas.gov	512-424-2686
CJIS Site Assistance Line			512-424-2500
Error Resolution Assistance Line			512-424-7256
CJIS Field Representative Assistance Line			512-424-2478

FINGERPRINT PROCESSING BUREAU

Walter Henson	Manager	walter.henson@dps.texas.gov	512-424-2260
Pat Molloy	Section Supervisor, Fingerprints	patricia.molloy@dps.texas.gov	512-424-7026
Randy Coppedge	Day Shift Supervisor, Fingerprints	randy.coppedge@dps.texas.gov	512-424-5709
Debbie Parsley	Day Shift Supervisor, Fingerprints	debbie.parsley@dps.texas.gov	512-424-5304
Kathy Parks	Evening Shift Supervisor, Fingerprints	kathy.parks@dps.texas.gov	512-424-5749
Toby Cross	Evening Shift Supervisor, Fingerprints	toby.cross@dps.texas.gov	512-424-5748
Hai Le	Midnight Shift Supervisor, Fingerprints	hai.le@dps.texas.gov	512-424-2408
Loann Garcia	LiveScan Coordinator	loann.garcia@dps.texas.gov	512-424-2409
Cheryl Sanchez	AFIS Project Assistant	cheryl.sanchez@dps.texas.gov	512-424-2089
24 hour Fingerprint Assistance Line			512-424-5248

CRIME INFORMATION BUREAU

Vacant	Manager	Vacant	512-424-2734
Diane Wells	TCIC Training Supervisor	diane.wells@dps.texas.gov	512-424-2982
Taffy Sweet	TCIC Audit Supervisor	taffy.sweet@dps.texas.gov	512-424-2897
Jill Gajkowski	TCIC Control Room Supervisor	jill.gajkowski@dps.texas.gov	512-424-2152

UNIFORM CRIME REPORTING BUREAU

Earl Adams	Manager	thomas.adams@dps.texas.gov	512-424-2418
UCR Assistance Line			512-424-2091
Rafael Martinez	Supervisor, UCR Field Reps	rafael.martinez@dps.texas.gov	512-424-7135
Tamika Ware	IBR Supervisor, UCR	tamika.ware@dps.texas.gov	512-424-2979

SEX OFFENDER REGISTRATION BUREAU

Vincent Castilleja	Manager	vincent.castilleja@dps.texas.gov	512-424-2279
Sex Offender Registration Assistance Line		txsor@dps.texas.gov	512-424-2800

TEXAS DATA EXCHANGE (TDEx) BUREAU

JC Villanueva	Manager	jc.villanueva@txdps.state.tx.us	512-424-7167
TDEx Assistance Line			512-424-2629