CR NEWS

HIGHLIGHTS:

Biometric Services Bureau (BSB) Electronic Arrest Reporting (EAR)/Livescan Dos and DON'Ts

When using a livescan to submit arrest data to Texas DPS it is important to remember the following dos and don'ts.

Livescan DOs and DON'Ts:

DO
- Check all return messages.
- Review reject messages, correct transaction, and resubmit.
- Use current offense codes (version 17).
- Transmit adult class C offenses.
- Use corresponding ADN for class C **(233)**, federal **(234)** offenses, and Family Violence class C **(235).**

DON'T
- Transmit out of state probation and paroles via livescan.
- Resubmit any transactions; verify with DPS first (Call 512-424-5248). For corrections or added charges, use the CJIS site: https://cch.dps.texas.gov or fax to 512-424-2476.
- Use offense code 99999999.
- Submit Juvenile class C offenses.
- Populate an arrest record with identification database on a name search from a DL search.

Access and Dissemination Bureau

FAST Location Status:
You can now find FAST Location Status updates on the TxDPS website, FAST Submission Locations | Department of Public Safety (texas.gov).This link provides updates on locations as they open and close. The report will be updated as closures change, Monday – Friday, excluding holidays. You can also email adbsupport@dps.texas.gov with any questions about FAST locations, concerns, or issues.

Newest Audit and Training Auditor – Carlos Ramirez:
Carlos Ramirez is the newest auditor within the Audit and Training Unit. He is originally from Dallas, TX but moved to central Texas in 2014. Carlos graduated from Texas State University with a Bachelor's in Criminal Justice. He began his career with the Department as a commercial vehicle inspector in Seguin, TX and promoted to the Auditor position in March of 2020. He is excited to bring his skills and experiences to ADB and hopes to continue to grow and learn from the Department.

Access and Dissemination Bureau (ADB) continued

<u>87th Legislative Session</u>

The 87th legislative session began on January 12, 2021. ADB has been actively monitoring bills relating to agency's access and requirements for dissemination of criminal history record information. ADB will keep agencies abreast of any changes in statute pertaining to access of criminal history information for non-criminal justice purposes.

CJIS Technical Security Office

A Fresh New Start for Security Planning

Technology advances rapidly, so do cybercriminals. Ransomware or targeted cyber-attacks can happen to anyone anywhere. Stay cyber alert. Protective measures are simple, cost-effective and immediately beneficial. Protective measures can help prevent ransomware from occurring in the first place. Prepare for a ransomware attack as though you can be a victim at any time. There are steps you can take to protect yourself and the agency.

Get to know your critical data. Know what data is most important to you and the agency. With your agency, personal information, or devices, you need to consider what can and cannot be replaced, what to budget for to recover the information or device loss, what you are willing to live without, and what must be kept safe.

Any data loss could limit the ability for the agency to conduct day-to-day activities. While one might think photos and other business documents are most important, it is worth considering other critical data to agency operations, for example: financial/transaction data, customer data (CJI, PII, contact information), communication platforms (access to and history of emails; if the agency is down, business email may be down too), calendars (appointments, hearings and bookings).

Update devices and turn on automatic updates as cybercriminals use known weaknesses to hack devices. System updates have security upgrades to patch these weaknesses. Always update the systems and applications when prompted with automatic updates turned on. Remember to apply security fixes and updates to network equipment too- VPN solutions, firewalls, routers, etc. See CJIS Security Policy requirements in Section 5.10.4.1.

Turning on two-factor authentication or advanced authentication increases cyber security. Two-factor authentication means there are two checks in place to prove identity before accessing an account. For example, you may need to supply an authentication code from an app and your password. This can make it more difficult for someone to access your files or account. See CJIS Security Policy requirements in Section 5.6.2.2.

Remember to use strong passwords and passphrases for your accounts. Longer is stronger and change them frequently. Unless you have a photographic memory and can recall everything, consider an encrypted password manager to help sort and organize them. See CJIS Security Policy requirements in Section 5.6.2.

Set up and perform regular backups. A backup is a digital copy of your most important information at rest (e.g. CJI data, evidence photos, or financial information) saved to an external storage device or to the cloud. For CJIS compliance ensure files are encrypted with FIPS 140-2 level encryption before CJI data transmits outside the device or entity. CJI cloud data must remain in the U.S. or an APB member country. The agency must retain control or management of the encryption keys. CJI data stored at rest must be a minimum FIPS 197 encryption. See specifics on encryption in CJIS Security Policy Section 5.10.1.2 and cloud requirements in Section 5.10.1.5.

Regular offline backups provide good resources to a quicker recovery. Backups are good; also remember to randomly test a file restore before a crisis to offer a little peace of mind the backup functions as expected. It would be too late during a needed recovery to find the files were not copied correctly, the files are corrupted or the last backup also contains ransomware. Ensure there are regular separate intervals of backups possibly in different locations or on different media platforms.

Implement access controls. Controlling who can access what on your devices is an important step to minimize unauthorized access. This can also limit the amount of data ransomware attacks can encrypt, steal, and delete. Give users access and control only to what they need by restricting administrator privileges. Don't share your login details for your accounts. Consider separation of duties. See CJIS Security Policy requirements in Section 5.5.

Turn on ransomware protection. Some operating systems offer ransomware, anti-virus and spam protection. Ensure this function is enabled to protect devices. Consider secondary software to bolster security. See CJIS Security Policy requirements in Section 5.10.4.2, 5.10.4.3, & 5.13.4.2.

Prepare a cyber emergency plan, disaster recovery plan or incident response plan. It is important these plans are easily accessible and known to all employees, especially in the event of a ransomware incident. Not only write the plans down, but treat them like fire drills. Run through the paces, try out those encrypted backups. Like regular drills, it becomes second nature and can lessen the stress when something does go awry. See CJIS Security Policy requirements in Section 5.3.2 & 5.13.5.

Remain vigilant and informed. Keep up security awareness training to stay current and informed on security measures. Multi-factor authentication, separation of duties, and user awareness training remain key and have to be supported by monitoring, patching, backup and incident response programs. Combining these steps adds defense in layers to help protect yourself and the agency.

 Questions?
We're here to help! Contact your CJIS Technical Auditor or the CJIS Security Committee at
Security.Committee@dps.texas.gov

- To report incidents, remember to first contact the agency's Terminal Agency Coordinator, Local Agency Security Officer & IT Support.
- Notify the Operations Intelligence Center (OIC) at 1-888-DPS-OIC0 (1-888-377-6420). The OIC will then contact the CJIS Technical Auditor on call to reach you.

Criminal History Record Information Processing (CHRIP) Bureau

CJIS Website Portal

Legislative Session

The 87th Legislative Session is in full swing. It has been a challenging session as everyone is working to stay safe while providing the same services to our community during the pandemic. As the session begins to wind down and legislation is signed, Crime Records will work to ensure any changes to reporting are fully implemented and communicated to all reporting agencies.

Websites

The Crime Records Division is in the process of modernizing the CJIS Website Portal. This modernization effort is aimed at increasing the efficiency and user friendliness of the CJIS Site. The new CJIS Site will only support the following browsers: Microsoft Edge, Chrome, Safari, and Firefox. Due to end of life of Internet Explorer 11, this browser is not recommended and will not be supported by the modernized CJIS Site. The implementation will be completed in phases, prioritized by CJIS Site functions. Currently NICS Indices Entry Reporting, the Juvenile Sealing Worklist, Latent Reporting, and some county's EDR functions have been converted to the new CJIS portal.

If you are using one of the applications on the new portal, it is important that you continue to log into the CJIS Site through the legacy portal, https://cch.dps.texas.gov/CJISAuth/. Use the tabs/links at the top of the page to navigate to the new portal. If the account on the legacy portal becomes Inactive, it can affect account functions on the new portal.

If you are new to the CJIS Website and are new to Electronic Disposition Reporting (EDR) via the online portal, please complete the Application for Access on the New Website Portal, https://cch.dps.texas.gov/les/.

If you have an existing CJIS Site Account, legacy site or new site, do not complete an Application for a New User for any purpose on either site. Contact GRP_CJIS_SITE@dps.texas.gov with the question or update to the existing account.

Criminal History Record Information Processing (CHRIP) Bureau continued

REACTIVATION: Needed when the account has been Deactivated or Locked due to no activity in 30 days.
- Send an email to GRP_CJIS_SITE@dps.texas.gov with a request to Reactivate/Unlock the account.
- The request is manually processed by a person at DPS.
- The User receives an email from cjis@dps.texas.gov that includes a link to reactivate the account. *The email is sent to the User ID (email address) associated with the account.
- **Use the link in that email.**
- The link will take the user to the Security Profile page of the account. On that page, verify the Site Image, Site Phrase, and the Security Questions and Answers. If the link takes you to any other web page, contact your local IT Department.
- Create/Enter a New Password, confirm the New Password.
- Click on 'Save Changes'.
- The page will then navigate to the Login page.
- Login with the User ID and the newly created Password.

TIPS:
- Deactivation/Locking after 30 days of Inactivity is an automatic process to stay in compliance with CJIS Security Policy. It cannot be stopped or delayed by anyone at DPS.
- Log into the account every two to three weeks, even if you do not complete any actions. This is the only way to reset the 30 day time clock.

PASSWORD RESET:
- Enter the User ID (email address) on the Login page, click 'Login'.
- Click on 'Forgot Password' under the password field.
- Answer the Security Question. Enter a New Password, Confirm the New Password.
- Page will navigate to the Login page. Login using the new password.

If you do not remember the answer to the security question:
- Click on 'Forgot your Answer?'
- This will generate an email to the Entity Administrator of your agency.
- The Entity Administrator will open the email and click on the link in that email.
- That will take the Entity Administrator to the CJIS Site, where they will click on 'Reset Now' in the upper right corner.
- The User receives an email from the Entity Administrator that includes a link to reset the password. *The email is sent to the User ID (email address) associated with the account.
- **Use the link in that email.**
- The link will take the user to the Security Profile page of the account. On that page, verify the Site Image, Site Phrase, and the Security Questions and Answers. If the link takes you to any other web page, contact your local IT Department.
- Create/Enter a New Password, confirm the New Password.
- Click on 'Save Changes'.
- The page will then navigate to the Login page.
- Login with the User ID and the newly created Password.

TIP:
-     If the Entity Administrator or the User do not receive the emails in the above situation, contact your local IT Department. There may be a firewall or email filter on the local network that is not allowing the emails to get to the intended Inbox.

- If there is not an Entity Administrator for your agency, the Password Reset request will be sent to the Website Administrator at DPS.
- The request is manually processed by a person at DPS.
- The User receives an email from cjis@dps.texas.gov that includes a link to reset the password. *The email is sent to the User ID (email address) associated with the account.
- **Use the link in that email.**
- The link will take the user to the Security Profile page of the account. On that page, verify the Site Image, Site Phrase, and the Security Questions and Answers. If the link takes you to any other web page, contact your local IT Department.
- Create/Enter a New Password, confirm the New Password.
- Click on 'Save Changes'.
- The page will then navigate to the Login page.
- Login with the User ID and the newly created Password.

Criminal History Record Information Processing (CHRIP) Bureau continued

TIP:
If you do not receive the email from cjis@dps.texas.gov, check your junk/spam email folder. If the email is not there, contact your local IT Department to add cjis@dps.texas.gov to the safe/allowed sender email list for your local network.

PASSWORDS MUST:
- Not be the same as the previous 10 passwords.
- Be at least 8 characters long.
- Contain a number and a special character.
- Passwords are Case Sensitive.

AUTHENTICATION CODE ENTRY:
Browser Authentication is required after every time internet cookies are cleared/deleted. If your browser settings are set to clear cookies at a regular interval (every time browser is closed, once a week, etc.) the Authentication is required the next time you access the CJIS Site.

It is important that you follow the steps below exactly when Authenticating a browser:
- Go to the login page, type in your User ID/email address.
- Page navigates to the Authentication page or opens it in a new tab.
- Important: **Leave that page open. Do Not close the Authentication page.** - If this page is closed before receiving and entering the PIN, then a new PIN will be generated and sent every time the page is opened. The data tables will not keep up with repeated PIN requests.
- Receive the Authentication PIN code via email.
- Enter that Authentication PIN and your password into the Authentication page.** - The Authentication webpage will time out after 15 minutes. If the code is not entered in that 15 minute window, a new code will be required.
- It should then navigate back to the Login page and/or give a message that the browser has been successfully authenticated.

ACCOUNTS:
- Do not share your password with anyone at any time, not even Entity or Website Administrators.
- Do not share an account with multiple users. To stay in compliance with FBI CJIS Security Policy, accounts are single user specific. This includes the email address/User ID on the account, only one person, the site user, can have access to that email account.
- There is no limit to the number of users an agency can have with individual accounts and individual email addresses/User IDs on the CJIS Website.

Crime Information Bureau (CIB)

2021 CIB Timeline

The Crime Information Bureau has a full plate in 2021! The continuous changes in legislature require updates to manuals and audit processes throughout the year. To kick things off, CIB is looking at the following projects for 2021:

- Training - Manual Revisions
- Training - Mini Virtual Courses
- TLETS Operations – Condition of Bond Form
- Control Room – LPR Process Improvement
- Audit – LPR Audit build, testing, and implementation

TCIC Training is faced with training the state's Law Enforcement personnel and DPS internal personnel on all policy & procedures regarding access and use of TCIC/NCIC information, TXGANG, TLETS, TAC responsibilities, and Associate Trainer training responsibilities/requirements. For the 2021 year, TCIC Training is adding the new virtual training requirements to the manuals and updating the legislative changes from the 87th Legislative session. With the retirement of MyTrain, Acadis has become the new trainingreporting system maintained by DPS Training Operations Division (TOD) which supports all TCIC/TLETS courses. In this transition, TCIC Training has learned, trained, and has trained and continues to train associate trainers on the use and reporting of Acadis.

Crime Information Bureau (CIB) continued

In addition to the manual updates, TCIC Training has created Virtual Mini Courses to assist agencies during the pandemic. Three new mini courses were created andare being staggered on their release to the user community. These three courses are TAC Admin, Security Roles/User Request Forms (URF), and nexTEST & Expiration Reports. These courses are half-day courses that do not provide the student any TCOLE Credit but helps them understand the processes they must complete for their agencies within the respective systems.

TLETS Staff works diligently to provide the Law Enforcement community with a secure and stable connection to this system. Enhancements and small user changes have improved connectivity and the system's functionality since the beginning of 2021. Recently a change caused a portion of the user community to lose connection for several days, up to a week, and was resolved with the help of all team membersand the TLETS Vendor.

Conditions of Bonds is just one of the many projects TLETS has implemented in the 2021 year. Bond conditions are court-imposed requirements that a defendant on pre-trial release must follow until his/her case is resolved. A judge signs an Order Setting Conditions of Bond/Release. These conditions can be re-visited or even challenged on appeal by the defendant. According to Article 17.40 of the Texas Code of Criminal Procedure, the Court has the authority to impose "any reasonable condition of bond related to the safety of a victim of the alleged offense or the safety of the community." A TCIC Conditions of Bond File has been established to create and modify bond condition records via TLETS using MKE EBN. EBN is a TCIC only file and will expire one year after the entry or last update date. Respondent information will include personal identifiers. Bond information will consist of bond condition, bond amount, bond remarks, issuing Court ORI, date issued, and the date of expiration. Optional fields such as protected person and vehicle information can be added. There will also be supplemental forms available to enter additional bond conditions, personal identifiers, vehicle, license, and miscellaneous information.

The TCIC Control Room provides 24/7/365 assistance to all law enforcement agencies throughout the United States. A local law enforcement agency can contact them for helpwith the entry/modification/clear/ and cancel of a record into TCIC/NCIC. TCIC Control Room is also responsible for the monthly validation, and message volume reports available through the TCIC Record Validation website. The TCIC Control Room has recently adjusted the validation date to help keep law enforcement agencies in compliance and validating their records promptly. Any agency that has failed to certify on time will be contacted by the TCIC Control Room staff for assistance.

For 2021, the TCIC Control Room has been tasked with assisting agencies with the License Plate Reader Program. The LPR Database shall consist of shared data from all participating local, state, and federal agencies, as well as TXDPS, captured data, of the followinginformation associated with a license plate captured by an LPR: license plate numbers; latitudeand longitude coordinates indicating where the plate was captured; date/time of the capture; and Originating Agency Identifier (ORI) information of the agency capturing the data.

The LPR Database is maintained, operated, and managed by TXDPS 24/7, 365 days a year. The Control Room has been tasked with streamlining the LPR process during the 2021 year, providing agencies with the information and assistance to submit reads and join the LPR Hotlist. Currently, the TCIC Control Room has been working with local agencies to bring them online and in compliance with the assistance of staff and vendors.

TCIC Audit unit conducts FBI mandated triennial audits on all law enforcement agencies throughout Texas that currently have access to TLETS/NLETS and TCIC/NCIC. Auditsare conducted online (virtually) and through a one-on-one interview with appropriate staff from the local law enforcement agency. The records reviewed during an audit are CCHlog, wanted persons, missing persons, stolen vehicles, protection orders, and TXGANG entries.

In 2021, TCIC Audit has been tasked to create a new audit for the License Plate Reader Program. The LPR Database shall consist of shared data from all participating local, state, and federal agencies, as well as TXDPS, captured data, of the following information associated with alicense plate captured by an LPR: license plate numbers; latitude and longitude coordinates indicating where the plate was captured; date/time of the capture; and Originating Agency Identifier (ORI) information of the agency capturing the data. TCIC Audit is responsible for creating an audit for this program considering the other agency audits conducted. TCIC Audit will complete the audit and test and implement the final audit in 2021.

Incident Based Reporting Bureau (IBRB)

<u>New look for DPS website?</u>

The Department has completed the website migration and has updated it with a new look and more user-friendly format; making it easier for the general public to navigate through the webpages to find the right department for their needs.

As part of this website update, the Incident-Based Reporting (IBR) Bureau made some changes on the DPS website to make it easier for law enforcement agencies (LEAs) to locate information. All of the changes can be viewed under <u>Law Enforcement Support > Crime Records Service</u>.

The Bureau continues to make an effort to maintain and keep all information updated pertaining to the UCR program.

The <u>Crime in Texas Public Portal</u> has also been updated with the new link for the updated website to access the most current <u>Crime in Texas (CIT) reports</u>.

Incident Based Reporting Bureau (IBRB)
TDEx

<u>Changes Ahead</u>
The new fiscal year has brought a new vendor for the Texas Data Exchange (TDEx). After more than a decade of partnering with Appriss to make TDEx available to our law enforcement and criminal justice community, the Department awarded a contract for a new TDEx implementation. What does that mean for the program in the future?

There will be no impact for agencies in regards to the use of the data collected. We moved away from Appriss' justiceXchange search portal (more commonly referred to by our users as the TDEx portal) in 2015 and directed users to the FBI's National Data Exchange (N-DEx). That data continues to be available in N-DEx.

The change for agencies will be in how we collect the data that will be shared and pushed to N-DEx. In the past, Appriss employed different methods to collect data from our contributors. Some agencies pushed their data out for collection via SFTP. Some had hardware sent to them to work as a data gateway. Appriss is currently working with those agencies to decommission the hardware or get it mailed back to Appriss headquarters.

With our new vendor, we will be employing a new data-contribution method. Agencies wishing to contribute data will be required to have the ability to convert their data to the new N-DEx IEPD 4.0 provided by the FBI. This, in conjunction with an Interface Control Document (ICD) currently being developed by DPG, will provide the information necessary for a contributing agency to get the data to DPS and then on to the FBI. The Department of Public Safety will be utilizing a data broker to accomplish this task.

Once fully implemented, agencies will submit their TDEx or NIBRS or both data sets once and have the data broker push data to N-DEx and the Uniform Crime Reporting (UCR) database. For agencies that choose to submit UCR data, the data broker will be able to pull National Incident-Based Reporting System (NIBRS) data from the submission and push it to UCR.

If you have any questions or you would like more information on the data broker submission process, please reach out to the TDEx Program office at tdex@dps.texas.gov

Incident Based Reporting Bureau (IBRB)
TDEx continued

Shift to XML

The TEXAS DPS has decided to change the way they collect data for inclusion in N-DEx.

No longer will the agency be asked to put hardware in their facilities. Instead, there will be an Interface Control Document (ICD) that will detail how to submit the data electronically. Along with the ICD, agencies will also be given a ReadMe file and a GetStarted file to help them.

All data shared through the Data Broker must be submitted in the FBI's N-DEx IEPD 4.0.

> **To access the N-DEx 4.0 IEPD:**
>
> N-DEx Website at https://www.fbi.gov/services/cjis/ndex
>
> N-DEx Helpdesk at ndex@leo.gov (request via e-mail)

The N-DEx IEPD 4.0 will have tables that detail the data that can be shared. Since participation is voluntary, there is no data that is required to be shared. However, there may be some contingency requirements (for example, if an agency were to decide to share arrestee name, then they may be required to also share DOB, HGT, WGT, etc.)

Future enhancements to the Data Broker will allow an agency to make one submission of data and have both N-DEx and NIBRS databases populated with their data.

If you have any questions, please reach out to our office at tdex@dps.texas.gov

Incident Based Reporting Bureau (IBRB)
Uniform Crime Reporting (UCR)

New Region 5 Field Representative
Leslie Dvorak is the newest Field Representative, to the Texas UCR IBR Training Staff for Region 5, Panhandle, TX. She is originally from Fort Collins, CO but moved to central Texas in 2016 to attend college. Leslie graduated from Texas State University with a Bachelor's in Criminal Justice. She was working in the public sector and began her career with the Department February of 2021. She is excited to assist the law enforcement agencies of Texas with training and learning about the Uniform Crime Reporting program and National Incident Based Reporting (NIBRS) reporting guidelines while learning herself about the Department.

Training Sessions
Please be looking for information about upcoming training sessions on our Acadis Portal and setting up your account online. Trainings will be on Introduction to NIBRS, Texas Mandated Reports, and How to Fix Your NIBRS Errors and many other great trainings. Our training staff is excited to see you all virtually in these trainings.   Some of these trainings will also be given TCOLE credit.

NIBRS Transition Update
Thank you everyone for your efforts to transition to NIBRS. As of April 22, 2021, 920 agencies representing more than 94.97% of the population of Texas are now submitting UCR data through the more-detailed NIBRS methodology.

Contact DPS by phone (512) 424-2091 or email NIBRS@dps.texas.gov if you are one of the agencies still working to get there or to let us know the challenges that prevented your transitioning to NIBRS in 2021.

Summary Agencies
January 1, 2021, FBI began to except only NIBRS data from agencies. Those agencies that have chosen not to transition to NIBRS have been moved to Non-Reporting status.

Texas-mandated Reporting
Agencies dropping out of the UCR program are still required to submit the Texas-mandated reporting (i.e. Family Violence, Sexual Assault, Drug Seized, and Hate Crime).

Contact DPS by phone at (512) 424-2091 or email UCR@dps.texas.gov to find out how to submit this information outside of the UCR submissions.

The FBI provided info in the UCR Program Quarterly: February 2021 (21-1) on page 11.

Three Group B Offenses have been eliminated

Effective January 1, 2021, the FBI eliminated three Group B offenses:
•	90A = Bad Checks
•	90E = Drunkenness (except Driving Under the Influence)
•	90H = Peeping Tom

If an agency reports a 90A, 90E, or a 90H offense, the FBI 's UCR computer system will automatically change the offense to a 90Z = All Other Offenses. Agencies reporting these offenses will not receive an error message. Agencies will not need to change their computer programming unless they want to eliminate the offenses in their databases as well.

This change was a result of the CJIS Advisory Policy Board (APB) meeting in December 2018, and the FBI Director approved this measure on May 5, 2019.

Texas DPS UCR Program Update:
1.	Texas DPS UCR Program will still accept 90A, 90E and 90H and will remain backwards compatible (with 3.0 thru 2019.2)
2.	As of 1/1/2021, the FBI will convert all of these offenses to 90Z.
3.	No changes are necessary at the local agency, as DPS will still accept these offenses as reported.
4.	The FBI reports will not match the local agency and state reports due to the FBI converting these Group B offenses.
***The FBI will include these changes in the future NIBRS specifications updates but has not provided a timeline.

Contact DPS by phone at (512) 424-2091 or email UCR@dps.texas.gov to find out how to submit this information outside of the UCR submissions.

Molly Jane's Law Virtual Training
TxDPS will be starting virtual trainings focused on the Molly Jane's Law and the Texas requirements. These trainings are estimated to be 2-hours in length and will begin mid-2021.

Accessing N-DEx
For local, county, and state law enforcement and criminal justice agencies, there are several ways to gain access to N-DEx. The most common way is to be granted access through the Law Enforcement Enterprise Portal (LEEP). Another option is to be a member of the Law Enforcement Information Exchange (LInX). Soon, members of the Regional Organized Crime Information Center (ROCIC) will also be able to access N-DEx.

More access points to N-DEx is a good thing. However, regardless of the access point, all agencies are subject to the triennial N-DEx audit. Whether you access N-DEx through LEEP, LInX, or ROCIC, your agency will need to provide a Point of Contact (POC) to our office for this purpose.

If your agency is a member of LInX or ROCIC, and you sponsor N-DEx access for other agencies in your area, then your agency will be responsible for the N-DEx usage of those other agencies and respond to any audit questions about them. If the sponsoring agency is not willing to answer audit questions for the agencies they sponsor access for, then those other agencies will need to provide TxDPS with their own POCs. This will ensure that all agencies are able to continue accessing the valuable data available in N-DEx and comply with program audit requirements.

Sex Offender Registration Bureau (SOR)

SOR 2021 Timeline

SOR is off to a busy start while ringing in the New Year! For SOR, last year also brought new responsibilities, innovative thinking, and the exceptional ability to adapt to day-to-day changes. 2021 started with a new set of challenges as the statewide freeze in February forced many employees out of their homes and workplaces. We understand that the storm had a devastating impact across many counties in Texas. We hope that our communities are healing and rebuilding, making for a better and safer future.

Our teams are busy improving processes, creating online training programs, implementing legislative mandates, and improving the statewide registry. These changes will effectively provide a more user-friendly environment for our law enforcement community, registry subscribers, and the general public. These and many more dynamic changes are taking place in our Bureau. 2021 and 2022 are shaping up to be eventful years as we acclimate to the new "normal" while still providing our users with the same excellent customer service, education, and resources you're used to receiving in years past.

Each of our SOR teams is comprised of dedicated staff who have worked diligently to provide our users with the latest updates, upcoming events, training, and SOR audit information in this article.

Sam Duncan and her team of Analysts and Investigators are currently working on multiple projects and updates to the registry resulting from triennial NSOR Audit Recommendations and requirements, legislative updates, and procedural updates. Offense Code data is being modified to promote uniformity and continuity in the user community. Data fields are being added to allow users to collect pertinent data sent to the National Sex Offender Registry, such as additional identifiers and phone numbers. The additional data will also assist agencies in completing accurate and complete annual validations of agency records. Users will soon receive an email notification when a registrant is removed from the secure site. This change will allow users to reconcile registrant records. An ethnicity field has been added to the high-risk offender postcards that get mailed out each week. Updates to the registry data structure are being tested so that offender photos can be sent to NSOR regardless of the size and format of the original submission. A QXS transaction will be tested through NCIC to support sync issues between TCIC/NCIC. This update will allow the user to view the results online. Our team of Investigators diligently reviews deregistration documents for users. They work directly with our legal team ensuring that each registrant's record is thoroughly inspected and verified. The Investigators also work closely with the Analysts to make improvements to the registry so that users have consistent access to current and accurate data.

Ryan McKenna and his team of Field Representatives (Reps) are preparing to begin auditing law enforcement agencies that enter data into the Texas Sex Offender Registry. Agencies will be audited on a triennial basis with audits, including records checked for accuracy, completeness, and validation procedures. The audits will provide users with tools, resources, and tips to aid in the accuracy and completeness of the entries in the registry. More information will be disseminated in the coming months about the audits, and users can expect ample notice from their Field Rep before the onsite audit itself. The Field Reps will also be collecting feedback from users, which will allow us to address your concerns and suggestions for future successful audits. The Field Rep will still be conducting online and classroom training in addition to the audits. They are realigning regions while adding the eighth region to support local law enforcement agencies' training and audit needs. Another change taking place in SOR is the creation of regional SOR Conferences. These smaller conferences will replace the biennial conference historically held in Galveston, Texas. Our Department sees the need to accommodate more agencies closer to user's duty stations and bringing pertinent information to them. The smaller conferences will present legislative updates, specialized training, and subject matter experts to agencies within regions that can accommodate large groups for one to two days. Neighboring agencies can send staff for all or specific portions of the conference. The Field Reps have already begun reaching out to agencies that could potentially host these smaller conferences. Please feel free to contact us if your agency would be interested in hosting a conference.

Alan Sustaita and his team of Technicians have undergone many procedural changes in the last year. Alan's team is responsible for ensuring your agency's phone calls, emails, and correspondence are responded to promptly. This past year, the group continued to process mail and streamline procedures, allowing for more online and paperless processes. The group rotates staff members into the office weekly. The technicians support the entire SOR team by processing hard copy correspondence such as subpoenas, death certificates, fingerprint cards, and deregistration forms. The SOR Technicians are also typically an agency's first point of contact through the 512-424-2800 number. The team successfully transitioned to working from home and rotating into the office while still providing support to our law enforcement community and the public. This talented team of individuals initiative and innovation will assist us in serving the state of Texas efficiently and comprehensively without sacrificing the excellent service our customers are used to receiving.

Do you have questions or need training?

We understand that the Sex Offender Registration material and procedures can get complicated at times. It's important to know that help is only a phone call or email away. If an agency reaches out seeking assistance we seize on the opportunity to offer help and provide training.

Our SOR Field Representatives are beginning to conduct in-person classes again throughout Texas. We will always consider safety first. Each agency request will be evaluated to ensure class sizes will accommodate social distancing practices and other COVID related precautions. Our trainers have also evolved and expanded our resources for conducting training using online platforms and telecommunications which allow us to continue to meet the training needs throughout the state.

Do you know who your regional Field Representative is?

If you have any questions about the Sex Offender Registry, the secure site or are interested in training, please contact your regional SOR Field Representative or contact us through the SOR Bureau main assistance line/email. Regional Trainer information is located at the end of this publication.

TxSOR@dps.texas.gov
SORB Main line: (512)424-2800
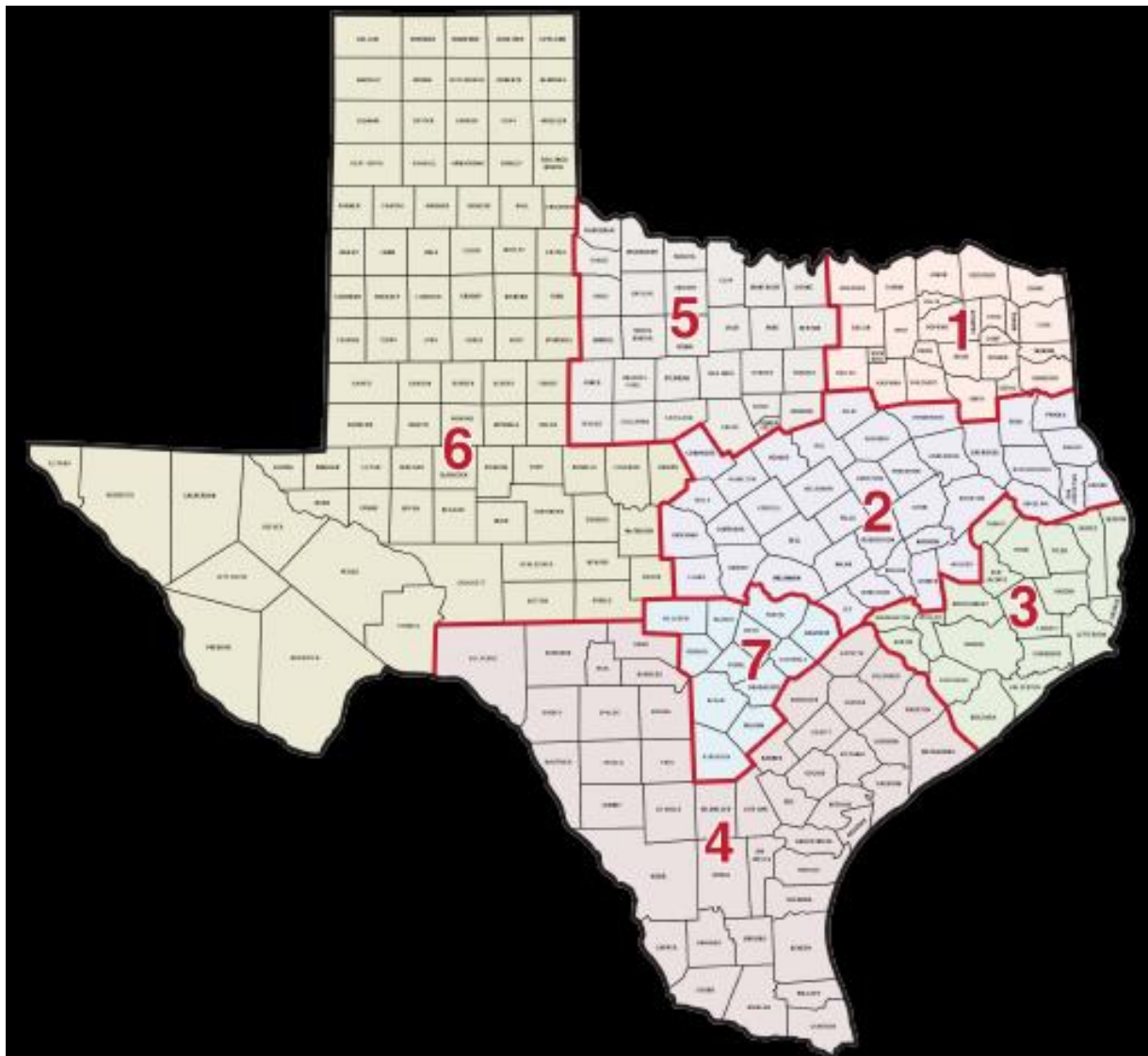
CRS Auditors/Field Representatives

CJIS Security Office

James Buggs	CJIS Technical Auditor		james.buggs@dps.texas.gov	512-424-7794
Vacant	CJIS Technical Auditor			
Dan Conte	CJIS Technical Auditor		daniel.conte@dps.texas.gov	512-424-7137
Enriquez Oswald	CJIS Technical Auditor		enriquez.oswald@dps.texas.gov	512-424-7914
William Frame	CJIS Technical Auditor		william.frame@dps.texas.gov	512-424-7401
James Gore	CJIS Technical Auditor		james.gore@dps.texas.gov	512-424-7911
Vacant	CJIS Technical Auditor			
Sonya Stell	CJIS Technical Auditor		sonya.stell@dps.texas.gov	512-424-2450
Deborah Wright	CJIS Technical Auditor		deborah.wright@dps.texas.gov	512-424-7876

ACCESS & DISSEMINATION BUREAU

Esmeralda "Essie" Romero	Non-Criminal Justice Auditor	Region 3	esmeralda.romero@dps.texas.gov	512-424-7367
Karen Germo	Non-Criminal Justice Auditor	Region 4	karen.germo@dps.texas.gov	512-424-7521
Alexandra Oyervides	Non-Criminal Justice Auditor	Region 5	alexandra.oyervides@dps.texas.gov	512-424-2855
Jane P. Armstrong	Non-Criminal Justice Auditor		jane.armstrong@dps.texas.gov	512-424-7399
Leatha Clark	Non-Criminal Justice Auditor		leatha.clark@dps.texas.gov	512-424-7403
Linda "Michelle" Hammonds	Non-Criminal Justice Auditor		linda.hammonds@dps.texas.gov	512-424-5019
Sharon Hill	Non-Criminal Justice Auditor		sharon.hill@dps.texas.gov	512-424-7920
Cristina Ibarra	Non-Criminal Justice Auditor		cristina.ibarra@dps.texas.gov	512-424-7943
Marcelo Sanchez	Non-Criminal Justice Auditor		marcelo.sanchez@dps.texas.gov	512-424-5444
Carlos Ramirez	Non-Criminal Justice Auditor		carlos.ramirez@dps.texas.gov	512-424-7384

CRIME INFORMATION BUREAU

Michelle Fisher	TCIC Auditor	michelle.fisher@dps.texas.gov	512-424-2240
Danna Garcia	TCIC Auditor	danna.garcia@dps.texas.gov	512-424-7886
Andrea Huntsberger	TCIC Auditor	andrea.huntsberger@dps.texas.gov	512-424-2095
Debra Hutson	TCIC Auditor	debra.hutson@dps.texas.gov	512-424-2232
Crystal Kaatz	TCIC Auditor	crystal.kaatz@dps.texas.gov	512-424-7244
Melanie McDermott	TCIC Auditor	melanie.mcdermott@dps.texas.gov	512-424-2252
Shelly Ramsey	TCIC Auditor	shelly.ramsey@dps.texas.gov	512-424-2260
Kimberly Simpson	TCIC Auditor	kimberly.simpson@dps.texas.gov	512-424-2246
Alma Castillo	TCIC Auditor	alma.castillo@dps.texas.gov	512-424-7637
Jeffery Castille	TCIC/TLETS Trainer	jeffery.castille@dps.texas.gov	512-424-7535
Jeffery Hammonds	TCIC/TLETS Trainer	jeffery.hammonds@dps.texas.gov	512-424-7861
Raymond Trejo	TCIC/TLETS Trainer	raymond.trejo@dps.texas.gov	512-424-2230
Melissa Walker	TCIC/TLETS Trainer	melissa.walker@dps.texas.gov	512-424-7309
Susan Whisenhunt	TCIC/TLETS Trainer	susan.whisenhunt@dps.texas.gov	512-424-2233

CRIMINAL HISTORY RECORD INFORMATION PROCESSING BUREAU

Andrew "Drew" Lambert	CJIS Auditor	Region 1	andrew.lambert@dps.texas.gov	903-255-5795
Jeff McIlhaney	CJIS Auditor	Region 2	jeff.mcilhaney@dps.texas.gov	979-776-3167
Craig Lopez	CJIS Auditor	Region 3	craig.lopez@dps.texas.gov	512-424-7614
Allante Smith	CJIS Auditor	Region 4	allante.smith@dps.texas.gov	512-424-7618
Orlando Gallegos	CJIS Auditor	Region 5	orlando.gallegos@dps.texas.gov	512-424-5539
Aaron Bonner	CJIS Auditor	Region 6	aaron.bonner@dps.texas.gov	512-424-5068
Austin Jordan	CJIS Auditor	Region 7	austin.jordan@dps.texas.gov	512-424-5973
Christopher Fiest	CJIS Auditor	Region 8	christopher.fiest@dps.texas.gov	512-424-7792
Anna Gay	CJIS Auditor	Region 9	anna.gay@dps.texas.gov	512-424-7552
	CJIS Auditor Assistant Line			512-424-2478

INCIDENT BASED REPORTING BUREAU

Jennifer "Jenn" Bushee	Field Service Rep	Region 1	jennifer.bushee@dps.texas.gov	512-424-2987
Elizabeth "Beth" Carroll	Field Service Rep	Region 2	elizabeth.carroll@dps.texas.gov	512-424-2569
Jaimee Mayes	Field Service Rep	Region 3	jaimee.mayes@dps.texas.gov	512-424-2460
Laurie Connally	Field Service Rep	Region 4	laurie.connally@dps.texas.gov	512-424-2025
Leslie Dvorak	Field Service Rep	Region 5	leslie.dvorak@dps.texas.gov	512-483-1625
Alejandra "Alex" Martinez	Field Service Rep	Region 6	alejandra.martinez@dps.texas.gov	512-424-2911

SEX OFFENDER REGISTRATION BUREAU

Tyon Cooper	SOR Field Rep	Region 1	tyon.cooper@dps.texas.gov	512-424-7615
Charles Francis	SOR Field Rep	Region 2	charles.francis@dps.texas.gov	512-424-2343
Christine Shuler	SOR Field Rep	Region 3	christine.shuler@dps.texas.gov	512-424-7047
Barry Ives	SOR Field Rep	Region 4	barry.ives@dps.texas.gov	512-424-5835
Irene Munoz	SOR Field Rep	Region 5	irene.munoz@dps.texas.gov	512-424-7650
Michael Holm	SOR Field Rep	Region 6	michael.holm@dps.texas.gov	512-424-7892
Rafael Martinez	SOR Field Rep	Region 7	rafael.martinez@dps.texas.gov	512-424-5578
Todd Hittner	SOR Field Rep		todd.hittner@dps.texas.gov	512-424-7885

DPS IDENTIFICATION SUPPLIES ORDER FORM

DPS IDENTIFICATION SUPPLIES ORDER FORM   CR-12 (Rev. 1/2021)

TO: CRIME RECORDS DIVISION   Date: _____
TEXAS DEPARTMENT OF PUBLIC SAFETY
PO BOX 4143
AUSTIN TX 78765-4143

Website address for FBI supply order: https://forms.fbi.gov/cjis-fingerprinting-supply-requisition-form

Please furnish the following supplies:

FORM NUMBER	DESCRIPTION	#PER PACKAGE	QUANTITY
CR-6	DPS Applicant Fingerprint Card*	250 per package	
CR-12	DPS Identification Supplies Order Form	100 per pad	
CR-23	Out of State Probation; Parole Supervision Fingerprint Card	single cards	
CR-26	Death Notice Form	100 per pad	
CR-42	Request for Criminal History Check	100 per pad	
CR-43	Adult Criminal History Reporting Form With Preprinted TRN and Fingerprint Card Attached*	100 per package	
CR-43	Adult Criminal History Reporting Form With Fingerprint Card Attached*	100 per package	
CR-43J	Juvenile Criminal History Reporting Form With Preprinted TRN and Fingerprint Card Attached*	100 per package	
CR-43J	Juvenile Criminal History Reporting Form With Fingerprint Card Attached*	100 per package	
CR-43P	Adult Probation Supervision Reporting Form With Preprinted TRN and Fingerprint Card Attached*	200 per package	
CR-43P	Adult Probation Supervision Reporting Form With Fingerprint Card Attached*	200 per package	
CR-44	Adult Supplemental Reporting Form	100 per package	
CR-44J	Juvenile Supplemental Reporting Form	100 per package	
CR-44S	Adult Supplemental Court Reporting Form	100 per pad	
CR-45	Adult DPS Fingerprint Card*	250 per package	
CR-45J	Juvenile DPS Fingerprint Card*	250 per package	
	Fingerprint Card Return Envelopes (For arresting agencies only)	100 per 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 months supply.
Please submit your order at least 4 weeks prior to depletion of your supplies.

NOTICE: Provide a complete shipping address.
PO Boxes are acceptable.

AGENCY _____

STREET ADDRESS _____

CITY_____ STATE_____ ZIP _____

ATTENTION _____

PHONE # (   ) _____

Direct questions concerning supply orders to (512) 424-2367
Fax# (512) 424-5599 • crssupplyorder@dps.texas.gov

CRS DIRECTORY

CRS MANAGEMENT

Michelle Farris	Assistant Chief	michelle.farris@dps.texas.gov	512-424-7659
Luz Dove	Deputy Administrator	luz.dove@dps.texas.gov	512-424-7964
Ursula Cook	Deputy Administrator	ursula.cook@dps.texas.gov	512-424-2407

CJIS Security Office

Stephen "Doc" Petty	Manager	stephen.petty@dps.texas.gov	512-424-7186

ACCESS & DISSEMINATION BUREAU

Tina Saenz	Manager	tina.saenz@dps.texas.gov	512-424-2078
Rochelle Torres	ADB Support Program Supervisor	rochelle.torres@dps.texas.gov	512-462-6171
Tanya Wilson	Program Supervisor, CHIU	tanya.wilson@dps.texas.gov	512-424-2523
Catalina Rodriguez-Combs	Fingerprint Services Supervisor	catalina.rodriquez-combs@dps.texas.gov	512-424-5894
Erika Stiggers	Supervisor, NCJU Training & Audit	erika.stiggers@dps.texas.gov	512-424-7927
Charlene Cain	CCH Internet Coordinator	charlene.cain@dps.texas.gov	512-424-2090
Jennifer Norton	Program Supervisor-Billing Unit	jennifer.norton@dps.texas.gov	512-424-2312
Lisa Garcia	CRS Billing Clerk	lisa.garcia@dps.texas.gov	512-424-2912
Barbara Rumley	CRS Billing Clerk	barbara.rumley@dps.texas.gov	512-424-2789
Assistance Line	Record Checks		512-424-5079
Assistance Line	Secure Site		512-424-2474
Tierra Heine	CJIS/JJIS Forms and Fingerprint Card Supplies	tierra.heine@dps.texas.gov	512-424-2367
Vacant	CJIS/JJIS Forms and Fingerprint Card Supplies		512-424-2367
	crssupplyorder@dps.texas.gov	**Fax order form to:**	**512-424-5599**

CRIMINAL HISTORY RECORD INFORMATION PROCESSING BUREAU

Holly Morris	Manager	holly.morris@dps.texas.gov	512-424-2686
John Morse	Supervisor, CJIS Field Support	john.morse@dps.texas.gov	512-424-5067
Brittany Chromcak	Supervisor, CCH Data Entry/Control Unit	brittany.chromcak@dps.texas.gov	512-424-7290
Nicole Berry-Moss	Day Shift Supervisor, CCH Data Entry/Control	nicole.berry-moss@dps.texas.gov	512-424-2216
Kerrie Herrera	Evening Shift Supervisor, CCH Data Entry/Control	kerrie.herrera@dps.texas.gov	512-424-2473
Cassandra Richey	EDR Coordinator	cassandra.richey@dps.texas.gov	512-424-2479
Vacant	Assistant EDR Coordinator	@dps.texas.gov	512-424-2500
Error Resolution Assistance Line			512-424-7256
CJIS Auditor Assistance Line			512-424-2478

BIOMETRIC SERVICES BUREAU

Loann Garcia	Manager	loann.garcia@dps.texas.gov	512-424-2409
Randy Coppedge	Day Fingerprint Shift Supervisor	randy.coppedge@dps.texas.gov	512-424-5709
Sandra Amaro	Day Fingerprint Shift Supervisor	sandra.amaro@dps.texas.gov	512-424-5748
Debbie Parsley	Evening Fingerprint Shift Supervisor	debbie.parsley@dps.texas.gov	512-424-5304
Mary Ann Gold	Midnight Fingerprint Shift Supervisor	mary.gold@dps.texas.gov	512-424-2408
Chrystal Davila	Biometric Coordinator	chrystal.davila@dps.texas.gov	512-424-7026
Chiquta Ruffin	Assistant Biometric Coordinator	chiquta.ruffin@dps.texas.gov	512-424-7404
Cathleen McClain	AFIS Coordinator	cathleen.mcclain@dps.texas.gov	512-424-2456
Madelyn Halley	Assistant AFIS Coordinator	madelyn.halley@dps.texas.gov	512-424-2089
24 hour Fingerprint Assistance Line			512-424-5248

CRIME INFORMATION BUREAU

Dax Roberts	Manager	dax.roberts@dps.texas.gov	512-424-5436
Margarete Perryman	TLETS Ops Supervisor	margarete.perryman@dps.texas.gov	512-424-7308
Matthew Foster	TCIC Training Supervisor	matthew.foster@dps.texas.gov	512-424-7888
Adina Decuire	TCIC Control Room Supervisor	adina.decuire@dps.texas.gov	512-424-2152
Sarah Bates	TCIC Audit Supervisor	sarah.Bates@dps.texas.gov	512-424-2253
TCIC/TLETS Audit Assistance		TCIC.audit@dps.texas.gov	512-424-2809
TCIC/TLETS Training Assistance		TCIC.training@dps.texas.gov	512-424-2832
24 hour TCIC Control Room- ORI Requests/Updates, Offline Requests & TxGang		TCIC.operations@dps.texas.gov	512-424-2088
Operations Information Center (OIC)		OIC@dps.texas.gov	512-424-2139

INCIDENT BASED REPORTING BUREAU

Brian Isaac	Manager	brian.isaac@dps.texas.gov	512-424-7893
JC Villanueva	TDEx Program Specialist	jc.villanueva@dps.texas.gov	512-424-7135
Esteban Perez	IBR Information Specialist	esteban.perez@dps.texas.gov	512-424-2307
Vacant	Use of Force Program Specialist	UoF@dps.texas.gov	512-424-2091
Maggie Walker	Supervisor, Training & Audit	maggie.walker@dps.texas.gov	512-424-0334
Elisa Hood-Waddle	Supervisor, IBR	elisa.hood-waddle@dps.texas.gov	512-424-2091

SEX OFFENDER REGISTRATION BUREAU

Sheila Vasquez	Manager	sheila.vasquez@dps.texas.gov	512-424-2279
Sam Duncan	Support Operations Supervisor	samantha.duncan@dps.texas.gov	512-424-7896
Alan Sustaita	SOR Program Supervisor	alan.sustaita@dps.texas.gov	512-424-5682
Ryan McKenna	SOR Supervisor	ryan.mckenna@dps.texas.gov	512-424-7366
Sex Offender Registration Assistance Line		txsor@dps.texas.gov	512-424-2800