THE CRIME RECORDS DIVISION NEWSLETTER

CR NEWS

Volume 25, Number 4
OCT.— DEC. 2020

HIGHLIGHTS:

CR NEWS is published by the Texas Department of Public Safety. Comments, suggestions and mailing list updates are welcome.

CR News MSC 0230
Attn: Heidi Paul
PO Box 4143
Austin, TX 78765-4143

Heidi.Paul@dps.texas.gov

Texas Department of Public Safety
Crime Records promoted to Division status

Effective January 1, 2021 Law Enforcement Support Division has been split into two separate Divisions, Crime Laboratory and Crime Records.

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.

A Fresh New Start for Security Planning continued

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 location. 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 TLETS 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.

Access and Dissemination Bureau (ADB)

New Audit and Training Supervisor – Erika Stiggers

Erika Stiggers began her employment with the Department on November 9, 2009 as an Examiner at the Dallas East Driver License Office (DLO). She worked in that office for about 2 years, then transferred to the Garland Mega Center. While at the Garland Mega Center, she applied and promoted to a Lead position for the Carrollton DLO in 2012. Erika was in the Lead position until about 2015. Once a Supervisor position opened in 2015, she applied and promoted into this position with multiple areas of coverage (Rockwall, Terrell, Canton office, Canton CDL, Emory, & Greenville). In 2017, Erika saw an opportunity to move closer to home so she transferred into a Supervisor position at the Garland Mega Center. She worked at this mega center until July 1, 2020. Erika worked closely with her Assistant Manager and Regional Manager on special projects, process improvements, employee morale, system upgrades, work schedules, House Bills, etc. In an effort to be closer to family, Erika transferred to the South Austin DLO on July 1, 2020. She applied for a position with the Access and Dissemination Bureau and obtained the Audit and Training Supervisor Position on December 1, 2020.

Denson Lobby (Austin,TX) Update:

As of November 1, 2020, the Denson Lobby is closed and is no longer a fingerprinting location. To maintain appointment availability IdentoGo has increased capacity at two other locations in Austin, 6448 E Highway 290, Ste. E-101, Austin, TX 78723-1041 and 7010 W Highway 71 Ste. 160, Austin, TX 78735-8335. The additional Austin locations will not accept walk-ins.

COVID Related Updates:

Due to the COVID-19 precautions applicants are experiencing longer than normal wait times for fingerprinting appointments around the state. We are working with our vendor to address the current situation, keeping in mind that the health and safety of the public and staff are our priority.

Biometric Services Bureau (BSB)
Electronic Arrest Reporting (EAR)/Livescan

Things to Keep In Mind When Purchasing a Livescan Device

When your agency is considering purchasing a livescan device, we recommend contacting the Biometric Coordinator prior to purchasing to verify if your agency can connect to the Texas DPS. Purchasing a livescan is a valuable investment for an agency because of the benefits of having a device. Such as, a speedy update to the Computerized Criminal History (CCH) and Interstate Identification Index (III), ten finger look up (TFLU), and inkless fingerprinting to name a few. There are also a few things to keep in mind when purchasing a livescan device:

- Does your agency plan on reporting class C arrests only, and/or class B and above?

If you are a Police Department, your agency wants to submit class B and above, and your agency central books with County SO, an agreement needs to be created between the County SO and your agency that the County SO will not submit on your agency's behalf.

- Ten Finger Look Up (TFLU) transactions are only a benefit for an agency that has a livescan that submits arrest data. The TFLU is a quick check to possibly identify someone who has a criminal history. There are additional transaction options such as:
  - Criminal Justice Applicant
  - Sex Offender Registration (SOR) Fingerprints
  - Deceased transactions fingerprinting to name of few.
- Does your agency plan to submit Criminal Justice Applicants and/or Sex Offender Registration (SOR) fingerprints?

If your agency wants to submit these type of transactions, a photo is required. Please ensure that your agency purchases a camera with your livescan device. Without a camera purchased that submits through the livescan device, DPS will not be able to setup your agency for Criminal Justice Applicants or SOR fingerprints.

We can provide your agency with a list of validated livescan vendors in Texas. Also, keep in mind you may choose to select any vendor from the FBI's Certified Product list and that vendor would need to go through a validation process with Texas DPS if the livescan will connect to DPS. You can email livescan@dps.texas.gov.

Criminal History Record Information Processing (CHRIP) Bureau

CJIS Website Portal

Crime Records 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, and Latent Reporting 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 get to the new portal. Do Not log directly into the new portal.

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

REACTIVATION: Needed when the account has been Deactivated due to no activity in 30 days.
- Send an email to GRP_CJIS_SITE@dps.texas.gov with a request to Reactivate 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.
- 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 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.
- 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 the Entity Administrator or the User do not receive the emails in the above situation, contact your local IT Department. There is 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.
- 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 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 any of your previous 10 passwords.
- Be at least 8 characters long.
- Contain a number and a special character.
- Password are Case Sensitive. Make sure to not have CAPS LOCK on when entering your password.

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.
- 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.
- There is no limit to the number of users an agency can have with individual accounts on the CJIS Website.

Incident Based Reporting (IBR) Bureau
Texas Data Exchange (T-DEx)

Zero Cycle N-DEx Audits

As we near the end of the N-DEx Audits Zero Cycle, it might be a good time to provide a look at how things are going. It's an opportunity for us to share common errors we are seeing and offer solutions to rectify those errors. It's part of why we have a Zero Cycle to begin with.

What exactly is a Zero Cycle audit? One way to look at it is as a trial run for each agency. We take a look to see how each N-DEx User Agency is utilizing the system and help them identify, and correct, any errors in their usage. The main purpose of the audit is so that User Agencies can demonstrate that they are able to account for WHY searches were conducted and that they were run for a legitimate reason. Because it is the first audit for the agency (Zero Cycle), there are no consequences for the misuse.

As stated above, we are near the end of the cycle. We have audited approximately 75% of our N-DEx User Agencies. So what are some of the most common errors we are seeing? There are a few types of errors that we are seeing most often.

Search Reason – Many searches are run with very vague information being provided here (i.e. "investigation", "criminal", "background", "suspect").

> ***Why is this an error?*** Because not enough information is being entered to allow the User to recall what the purpose of the search was.
>
> ***What case was being worked?*** If a user is unable to recall the case, then we cannot determine if the search was for a legitimate purpose.

The Search Reason provides the user the opportunity to insert information that will help them remember why the search was conducted in the event that they are audited. Case numbers, investigation type with month and year, and other pertinent information will be of use to the individual who conducts the search.

Use Code – There are three main codes available.

1. **Use Code C** should be used when conducting a search for a criminal investigation.
2. **Use Code J** should be used when conducting a background check on a prospective employee for the user's agency (background checks should not be conducted for contractors, ride-along requests, or on behalf of another agency or entity).
3. **Use Code A** allows an agency's administrator to audit their records for accuracy.

Most searches are run using Use Code C, regardless of the actual reason for the search.

Non-Authorized Searches – We have found that searches are being conducted on friends, family, celebrities, co-workers, and on one's self. This seems to happen most often when a user is first granted access to N-DEx. These types of searches are never permissible and could lead to a user losing their access to N-DEx.

If your agency has already been audited in the Zero Cycle, then you have probably already heard much of what is listed above. If your agency has not yet been audited, these are some of the things you can expect our audit team to be looking at.

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

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

NIBRS Transition Update
Thank you everyone for your efforts to transition to NIBRS. Agencies representing more than 90% 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 transition, so we can coordinate in 2021.

Summary Agencies
Participating UCR agencies that have not transitioned to NIBRS by the FBI's deadline of January 1, 2021 will need to finalize their 2020 data. Only NIBRS data will be accepted by the FBI starting with 2021 incidents. These agencies will be shifted to Non-Reporting status after the year-end closeout of 2020 data (deadline 2/16/2021).

Texas-mandated Reporting
Agencies opting-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.

Incident Based Reporting (IBR) Bureau
Violent Criminal Apprehension Program (ViCAP)

FBI & DPS Host Collaborative Training
More training is coming in the spring and the FBI ViCAP team is partnering again with TxDPS to present a half-day virtual training on the ViCAP national data collection, as well as the Texas Molly Jane's Law and requirements on 3/9/2021 with more sessions to follow.

Contact TxDPS by phone (512) 424-2091 or email ViCAP@dps.texas.gov for more information.

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 in early 2021.

Contact the TxDPS ViCAP program by phone at (512) 424-2091 or email ViCAP@dps.texas.gov for more information.

Sex Offender Registration (SOR) Bureau

At what point does a **L**aw **E**nforcement Agency get involved with the **DEREGISTRATION PROCESS**, also, known as the **EARLY TERMINATION PROGRAM**.

Texas law allows for individuals on the Sex Offender Registry to petition to have their names removed from the registry if they meet certain conditions. This is called "deregistration". Although DPS does have a minor role in deregistration, a registrant's initial application process starts at the Council on Sex Offender Treatment (CSOT), an entity under the Health and Human Service Commission (HHSC), which has an active role in the Deregistration process.

Sex Offender Registration (SOR) Bureau continued

There's a few things, according to Chapter 62 Subchapter I CCP, that a person needs to do in order to receive a court order terminating their registration duty.

Step:

1) **Go to the CSOT Deregistration page (link below)**, and follow the steps to determine if the person is eligible for Deregistration.
    a. There is a checklist to help guide them.
        i. There is a whole page that explains what documentation must be provided to CSOT.
        ii. It explains the fee for the administrative review that will be paid to CSOT.
    b. Then they need to follow the procedural steps
        i. Confirm only 1 reportable sex offense exists
            1. If more than 1, then the person is in-eligible
        ii. Confirm that their duty to register as defined by TX exceeds the minimum registration duty required under federal law (SORNA).
    c. They can visit the public sex offender registration site (look under Additional Resources) to see if their offense exceeds the federal minimum registration duty. Then submit all information (court documents and background checks) required with the Initial Eligibility form and payment.
    d. If they meet all of the criteria, then CSOT will provide the registrant with a list of qualified Deregistration Specialists.
2) **The registrant will have to arrange, and pay for the Deregistration Specialist to conduct an Individual Risk Assessment.**
    a. The deregistration specialist sends their assessment report back to CSOT
    b. CSOT will certify the assessment report and send it to the registrant or their attorney.
3) Once they've received their individual risk assessment they can file a **motion for early termination of sex offender registration with the court where they were convicted**.
4) If the **court issues an Order Granting Early Termination**, then they will bring that motion and order, to the law enforcement agency that verifies their registration.
5) **Than the Law Enforcement Agency will complete and send a CR-33 Request for Removal**, including all documents, to DPS Sex Offender Registration Bureau.
6) **SORB will review the order** and process the removal if all criteria of Subchapter I have been met.

As you can see, Law Enforcement agencies don't come into this until nearly the end of the whole process. The registrant (or his attorney) is responsible for everything before it gets to your door. And SORB doesn't come in until the final step.

Here's a link to all of the important websites with this information.

Chapter 62, Subchapter I, TX C.C.P. - http://www.statutes.legis.state.tx.us/Docs/CR/htm/CR.62.htm#62.401

Council on Sex Offender Treatment - https://hhs.texas.gov/doing-business-hhs/licensing-credentialing-regulation/professional-licensing-certification-unit/council-sex-offender-treatment/deregistration

Step-by-Step Guide to Deregistration - https://hhs.texas.gov/sites/default/files/documents/doing-business-with-hhs/licensing-credentialing-regulation/csot/csot-deregistration-step-by-step.pdf

DPS Public Sex Offender Registration Website - https://records.txdps.state.tx.us/SexOffenderRegistry

Texas Offenses Tiered Under the Federal Adam Walsh Act – is on the DPS Public Sex Offender Registration Website under "Additional Resources"

CRD Auditors/Field Representatives

CJIS Security Office

James Buggs	CJIS Technical Auditor	james.buggs@dps.texas.gov	512-424-7794
Jeannette Cardenas	CJIS Technical Auditor	Jeannette.cardenas@dps.texas.gov	512-424-7910
Dan Conte	Lead 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
Linda Sims	CJIS Technical Auditor	linda.sims@dps.texas.gov	512-424-2937
Sonya Stell	CJIS Technical Auditor	sonya.stell@dps.texas.gov	512-424-2450
Deborah Wright	Lead 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
Alma Castillo	Non-Criminal Justice Auditor		alma.castillo@dps.texas.gov	512-424-5391
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
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	512-424-2841
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
Vacant	SOR Field Rep		@dps.texas.gov	512-424-2800

DPS IDENTIFICATION SUPPLIES ORDER FORM

CR-12 (Rev.11/16)

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

Date: _____

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

Please furnish the following supplies:

FORM NUMBER	DESCRIPTION	COUNT PER PKG	QUANTITY ORDERED
CR-6	DPS Applicant Fingerprint Card*	250 p/pkg	
CR-12	DPS Identification Supplies Order Form	100 p/pad	
CR-23	Out of State Probation/Parole Supervision Fingerprint 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** Preprinted TRN and Fingerprint Card Attached*	200 p/pkg	
CR-43P	Adult Probation Supervision Reporting Form **with** Fingerprint Card Attached*	200 p/pkg	
CR-44	Adult Supplemental 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	
	Fingerprint Card Return Envelopes (For arresting agencies 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 months' supply.
Please submit order at least 4 weeks prior to depletion of your supplies.

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

AGENCY
_____

STREEET ADDRESS
_____

CITY _____STATE _____ZIP

CRD DIRECTORY

CRD MANAGEMENT

Michelle Farris	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
Deborah Wright	Lead Technical Auditor	deborah.wright@dps.texas.gov	512-424-7876
Dan Conte	Lead Technical Auditor	daniel.conte@dps.texas.gov	512-424-7137

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, ADB	tanya.wilson@dps.texas.gov	512-424-2523
Catalina Rodriguez-Combs	Fingerprint Services Supervisor	catalina.rodriquez-combs@dps.texas.gov	512-424-5894
Vacant	Supervisor, NCJU Training & Audit		512-424-5105
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
Vacant	Customer Service Rep		512-424-7111
Lisa Garcia	CRS Billing Clerk	lisa.garcia@dps.texas.gov	512-424-2912
Vacant	CRS Billing Clerk		512-424-2936
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
Lenore Hemstreet	Evening Shift Supervisor, CCH Data Entry/Control	lenore.hemstreet@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