TEXAS DEPARTMENT OF PUBLIC SAFETY

5805 N LAMAR BLVD • BOX 4087 • AUSTIN, TEXAS 78773-0001
512/424-2000
www.dps.texas.gov

STEVEN C. McCRAW
DIRECTOR
FREEMAN F. MARTIN
DWIGHT D. MATHIS
JEOFF WILLIAMS
DEPUTY DIRECTORS

COMMISSION
STEVEN P. MACH, CHAIRMAN
NELDA L. BLAIR
STEVE H. STODGHILL
DALE WAINWRIGHT

Policy Statement – Texas CJIS Systems Access
Revised 03/16/2022

BACKGROUND

The Department of Public Safety (DPS) is the CJIS Systems Agency (CSA) for Texas. As the CSA, DPS has applied the rules contained within the *CJIS Security Policy* for access to the Texas Law Enforcement Telecommunications System (TLETS) and associated systems which include the Texas Crime Information Center (TCIC) and the Texas Computerized Criminal History (CCH) file and others. The FBI's *CJIS Security Policy* provides a procedure for conducting national fingerprint-based record checks on all personnel having unescorted access to unencrypted CJI including those with only physical or logical access to devices that store, process, or transmit unencrypted CJI. These record checks shall be conducted prior to granting access to CJI for all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas (during times of CJI processing). If a felony conviction exists, the hiring authority shall deny systems access. If a criminal record of any other kind exists, systems access shall be denied until the CJIS Systems Officer (CSO) or their official designee reviews the matter to determine if systems access is appropriate. If the person appears to be a fugitive (Outstanding arrest Warrant) or appears to have an arrest history without conviction for a felony or serious misdemeanor, the CSO or official designee shall review the matter to determine if systems access is appropriate. The procedure further provides that if the CSO or designee determines that FBI CJIS system access by the applicant "would not be in the public interest", access will be denied, and the agency will be notified of the denial in writing.

Local agency administrators may authorize or deny access to FBI and DPS systems as stated in this policy. Any questions regarding the application of this policy should be referred to the Manager of the CJIS Security Office, or the state's CSO.

POLICY (TERMINAL/NETWORK ACCESS)

Individuals that have terminal access or access to any equipment that stores, processes, or transmits Texas or National CJIS Systems data are required to pass a national fingerprint-based background check. This includes contractors covered by a security addendum, as well as City, County, and other governmental IT staff under a management control agreement with the criminal justice agency. The Department considers any TCIC/NCIC record information and CCH/III information as criminal justice data. Information derived from the Driver License system or the Vehicle Registration system via TLETS contains personal and private information that could be protected by federal or state statute but not by the FBI Security policy.

When the local criminal justice agency is reviewing an individual's criminal history record information, please note that the Department considers a deferred adjudication as a conviction for screening purposes.

To establish a practical process for screening in Texas that is consistent with the CJIS Security Policy requirements, DPS is simply applying the criminal history background screening requirements within the Texas Commission on Law Enforcement (TCOLE) peace officer licensing rules to persons requesting access to the Texas and national CJIS systems.

For persons who are peace officers:
The Department will allow access to DPS and FBI systems when a peace officer has a valid active license from TCOLE. This means regardless of any criminal history background, the Department will not revoke a peace officer's access as long as the TCOLE license remains valid and active.

For persons who are not peace officers:
The Department will consider TCOLE peace officer criminal history screening rules to determine eligibility for systems access. The complete rules can be found in Title 37, Texas Administrative Code, Chapter 217. The chart enclosed represents the TCOLE rules utilized by the Department for access to the CJIS systems.

The DPS does not need to review every applicant. Local agency administrators may authorize or deny access to FBI and DPS systems as stated above. In instances where there are questions, please contact the Manager of the CJIS Security Office, Crime Records Division, as stated above.

The local agency administrator (i.e., Chief, Sheriff, or their equivalent) may request a wavier that would allow access to the DPS/FBI systems. To qualify for a waiver, an individual must have been convicted or placed on community supervision for a Class B misdemeanor at least five (5) years prior to the application. The agency head must articulate in writing the mitigating circumstances that exist with the case and must attest to the value of the individual to the criminal justice community. The request shall also include a statement that the public interest would be served by reducing the denial period. These requests shall be addressed to the CJIS Systems Officer (CSO) at the following resource address:

security.committee@dps.texas.gov

Should the TCOLE licensing rules be amended in the future, the Department will examine the rules as amended and determine whether they remain an appropriate measure of an individual's access to DPS and FBI systems.

POLICY (HARD-COPY ACCESS ONLY)

To make the State of Texas fingerprint-based criminal history background check requirements consistent with the national standards as expressed in the CJIS Security Policy, it is no longer necessary to process a national fingerprint-based background check for those criminal justice agency employees that only have access to "hard-copy" criminal justice data. All other rules apply to these hard-copy only employees, the only change is that fingerprint-based criminal history background checks will not be necessary. Of course, agencies are still authorized to run these searches if they elect to do so.

Those employees with terminal access or access to any equipment that stores, processes, or transmits

criminal justice data will still be required to pass a national fingerprint-based background check. Also, this change does not apply to contractors covered by a security addendum. Passing a national fingerprint-based background check will remain a requirement of all contractor employees covered by a security addendum. City, county, and other governmental IT staff under a management control agreement with the criminal justice agency would still need to have a national fingerprint-based background check done.

The only change is for criminal justice agency employees that in the course of performing their job duties come into contact with hard-copy printouts of criminal justice data. This access to paper-only information will not require them to be fingerprinted. All other rules regarding dissemination of criminal histories, the care of keeping this information private, and securely storing this information when applicable will still need to be followed by these employees. A corresponding change was made to the background check requirements for non-criminal justice agencies with statutory access to the Texas and national criminal history record information for purposes such as licensing, employment, and volunteers.

If you have any questions regarding the "hard-copy" access policy, please contact Stephen Petty, CJIS Information Security Officer, at (512) 424-7186 or by email at stephen.petty@dps.texas.gov