



# CJIS SECURITY LISTSERV

## TXDPS Crime Records Division – Compliance & Training Bureau

Website: <https://www.dps.texas.gov/section/crime-records/welcome-tx-cjis-security-office>  
Don't feel comfortable clicking links? Copy and paste the URL into a new browser.

# Why Fire Department(FD) and Emergency Medical Services(EMS) personnel are not granted unrestricted access to Criminal Justice Information(CJI).

**The access and use of CJI are governed by strict federal guidelines outlined in the FBI's Criminal Justice Information Services (CJIS) Security Policy (CJISSECPOL).**

### **Reasons and clarification of the CJISSECPOL's restrictions:**

#### **1. Legal and Policy Framework**

- CJI access is explicitly limited to entities involved in the administration of justice, including law enforcement agencies, courts, and specific authorized personnel.
- Fire departments and EMS personnel, while critical to emergency response, do not meet the definition of entities directly involved in criminal justice processes, such as investigating crimes, enforcing the law, or prosecuting offenders.
- Expanding access beyond authorized personnel would violate these legal frameworks and could result in compliance failures, liability risks, and potential federal enforcement actions.

#### **2. Role-Specific Requirements**

CJI is meant to support criminal justice activities, such as:

- Conducting criminal background checks
- Supporting ongoing investigations
- Enhancing officer and public safety during law enforcement actions

Firefighters and EMS personnel focus on **emergency medical care, fire suppression, and rescue operations**. This work is invaluable but is not aligned with the intended purpose of CJI access.

#### **3. Security and Privacy Concerns**

CJI contains highly sensitive information, including criminal history records, arrest warrants, and ongoing investigation details. To ensure this data remains protected:

- Access is restricted to those who are trained in safeguarding CJI under the CJISSECPOL.
- All authorized personnel must undergo state of residency and national fingerprint-based record checks and annual training to maintain compliance with the CJISSECPOL.

Providing access to non-law enforcement personnel would create significant privacy risks. Unauthorized disclosure could harm individuals, compromise investigations, or lead to legal consequences for the agency responsible.

#### **4. Operational Segregation of Duties**

The separation of roles between fire, EMS, and law enforcement is intentional and legally enforced to:

- Preserve the integrity of sensitive criminal justice processes.
- Prevent conflicts of interest or misuse of information.

This does not mean that information sharing is prohibited; rather, it is designed to ensure that any data shared between law enforcement and Fire/EMS agencies happens in a controlled, lawful, and purposeful manner. For example, relevant situational details can still be communicated through authorized law enforcement channels when appropriate.

#### **5. Collaboration Through Alternative Means**

While direct access to CJI is not permitted, there are mechanisms in place to ensure that Fire and EMS personnel can still collaborate effectively with law enforcement, particularly during emergencies. These include:

- Information sharing through incident-specific protocols: For example, law enforcement can provide situational awareness during active shooter scenarios, hazardous materials incidents, or other emergencies requiring joint agency response.
- Law enforcement liaison roles: Many agencies designate points of contact for inter-agency communication, ensuring necessary information is shared without granting unrestricted access to CJI.

By maintaining compliance with CJIS policies, we protect not only the sensitive information but also the integrity of the collaboration between public safety agencies.

We deeply value the critical role of the Fire Department and EMS in ensuring community safety and recognize the importance of inter-agency collaboration. However, CJI access must remain restricted to ensure compliance with federal regulations, uphold data security, and minimize risk to all agencies involved.

#### **Additional references:**

##### **Texas Government Codes:**

##### **Sec. 411.082. DEFINITIONS. In this subchapter:**

- (1) "Administration of criminal justice" has the meaning assigned by Article [66.001](#), Code of Criminal Procedure.
  - (1-a) "Applicant" means an individual who submits an application for employment, licensure, certification, or registration that requires the department to conduct a background check using criminal history record information.
  - (1-b) "Application" means an application submitted by hard copy or electronically for employment, licensure, certification, or registration that requires the department to conduct a background check using criminal history record information.
- (2) "Criminal history record information" means information collected about a person by a criminal justice agency that consists of identifiable descriptions and notations of arrests, detentions, indictments, information's, and other formal criminal charges and their dispositions. The term does not include:
  - (A) identification information, including fingerprint records, to the extent that the identification information does not indicate involvement of the person in the criminal justice system; or
  - (B) driving record information maintained by the department under Subchapter [C](#), Chapter [521](#), Transportation Code.
- (3) "Criminal justice agency" means:
  - (A) a federal or state agency that is engaged in the administration of criminal justice under a statute or executive order and that allocates a substantial portion of its annual budget to the administration of criminal justice; or

(B) a nongovernmental railroad or campus police department that has obtained an originating agency identifier from the Federal Bureau of Investigation.

(4) "Criminal justice purpose" means:

(A) an activity that is included in the administration of criminal justice; or

(B) screening of applicants for employment with a criminal justice agency.

(5) "Office of capital and forensic writs" means the office of capital and forensic writs established under Subchapter B, Chapter 78.

(6) "Public defender's office" has the meaning assigned by Article 26.044(a), Code of Criminal Procedure.

#### **Sec. 411.083. DISSEMINATION OF CRIMINAL HISTORY RECORD INFORMATION.**

(a) Criminal history record information maintained by the department is confidential information for the use of the department and, except as provided by this subchapter or Subchapter E-1, may not be disseminated by the department.

(b) The department shall grant access to criminal history record information to:

(1) criminal justice agencies;

(2) noncriminal justice agencies authorized by federal statute or executive order or by state statute to receive criminal history record information;

(3) the person who is the subject of the criminal history record information;

(4) a person, including a research organization or public or private institution of higher education, working on a research or statistical project that is related to the administration of criminal justice and approved by the department and that:

(A) is funded in whole or in part by a criminal justice grant or government funds; or

(B) meets the requirements of Part 22, Title 28, Code of Federal Regulations;

(5) an individual or an agency that has a specific agreement with a criminal justice agency to provide services required for the administration of criminal justice under that agreement, if the agreement:

(A) specifically authorizes access to information;

(B) limits the use of information to the purposes for which it is given

#### **Sec. 411.089. ACCESS TO CRIMINAL HISTORY RECORD INFORMATION: CRIMINAL JUSTICE AGENCY.**

(a) A criminal justice agency is entitled to obtain from the department any criminal history record information maintained by the department about a person.

(b) Criminal history record information obtained under Subsection (a) may be released by the criminal justice agency:

(1) to any other criminal justice agency, if such release is for a criminal justice purpose; and

(2) through audio response terminals and radio devices, whether digital or voice, if such dissemination is in accordance with rules promulgated by the department.

#### **TCIC/NLETS Operating Manual:**

System Access Policies

##### **TLETS/NLETS Security & Access Policy**

Texas Law Enforcement Telecommunications System (TLETS) and the International Justice and Public Safety Network (NLETS) are designed exclusively for use by criminal justice agencies in

conducting their lawfully authorized duties within their respective jurisdictions. Data obtained over these systems may only be disseminated to criminal justice agencies as defined by state statute and federal regulations.

Each agency must ensure that TLETS terminals and/or terminals on local systems, which have access to TLETS, are secure from unauthorized use.....

#### **NCIC Dissemination Policies**

The data stored in the NCIC system and the Interstate Identification Index (III) files are documented criminal justice information and must be protected to ensure correct, legal, and efficient dissemination and use. It is incumbent upon every agency operating an NCIC terminal to implement the necessary procedures to make that terminal secure from any unauthorized use. Departure from this responsibility warrants the removal of the offending terminal from further NCIC participation. Information can be obtained from NCIC and the III files both directly and indirectly. Direct access is terminal access and dissemination within that terminal agency. Indirect access is non-terminal access outside of an agency with direct access. The individual receiving a request

for criminal justice information must ensure the person requesting the information is authorized to receive the data. Unauthorized request or receipt of NCIC material could result in administrative or criminal proceedings brought against the agencies and/or the individuals involved.

Thank you for subscribing to the CJIS Security Office Technical listserv.

We truly appreciate you.