Crime Records Services
Access and Dissemination Bureau

Susie Dial-Herrera, Supervisor
Access & Dissemination Unit
# Definitions

<table>
<thead>
<tr>
<th><strong>CHRI:</strong></th>
<th>Criminal History Record Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CJI:</strong></td>
<td>Criminal Justice Information</td>
</tr>
<tr>
<td><strong>Access:</strong></td>
<td>The ability to receive, view, or discuss CHRI</td>
</tr>
<tr>
<td><strong>CJIS Security Policy:</strong></td>
<td>A policy regarding CHRI enforced by the FBI to which all states and authorized private entities must adhere</td>
</tr>
</tbody>
</table>
TxDPS Crime Records Service
Secure Website

Computerized Criminal History Search
Search for individuals in the Computerized Criminal History System (CCH). Access is restricted to authorized Entities.

Texas Sex Offender Access for Criminal Justice Users
Allows local law enforcement agencies to submit and search information for Texas Sex Offender Registry.

Consolidated Response
Consolidated Response provides the fingerprint results from the DPS and the FBI AFIS/Criminal History Systems that have been processed through Fingerprint Applicant Services of Texas (FAST).

F.A.C.T. Clearinghouse
The FACT Clearinghouse is a repository of the DPS and the FBI fingerprint-based criminal history results. Only persons processed through Fingerprint Applicant Services of Texas (FAST) are eligible for FACT.

Uniform Crime Reporting - Summary
The objective of the Uniform Crime Reporting program is to produce reliable crime statistics for law enforcement administration, operation, and management. This information is also available as a measure of the fluctuations in the type and volume of crime in Texas.

Uniform Crime Reporting - Incident Based Reporting (NIBRS)
Incident-based reporting is a more detailed form of UCR than Summary. It requires an agency to have a records management system that produces data sets in NIBRS format. As with Summary, the objective is to produce reliable statistics to measure criminal activity.

Related Services and Websites
What access does this system allow...

• **Criminal History Search**
  - **Name-based Searches**
    Search for individuals in the Computerized Criminal History System (CCH). Access is restricted to authorized Entities.

• **F.A.C.T. Clearinghouse**
  - **Fingerprint results & searches**
    The FACT Clearinghouse is a repository of the DPS and the FBI fingerprint-based criminal history results. Only persons processed through Fingerprint Applicant Services of Texas (FAST) are eligible for FACT.
Eligibility

- Criminal justice agencies
- Entities identified in the Government Code for background searches for specific non-criminal justice purposes
- Research purposes
Legislatively Authorized Government Entities and Criminal Justice Agencies:

- Cities – employment and licensing
- Counties – employment and licensing
- School Districts
- Higher Education
- Hospitals and Hospital District
- Public Transportation
- Fire Departments
- Regional Toll way Authorities
- State Agencies
- County & District Clerks
- Juvenile Probation
- Adult Probation

Legislatively Authorized Private Entities
What are the requirements?

- A criminal justice and non-criminal justice entity legislatively authorized by Chapter 411, Subchapter F of the Texas Government Code or other Texas law to received criminal history record information from the Department of Public Safety may access the DPS Secure Site.
Omnixx vs. Secure Site

- Criminal Justice Agencies only
- Texas and National Criminal Histories
- Name based only
- Warrants/Stolen Vehicles/Missing Persons/Protective Orders/ etc.

- Criminal Justice/Non-criminal Justice Agencies
- Name based searches Texas only
- Live Texas fingerprint & static FBI results
The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for the access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.
Hardware/Software

Minimum requirements:

• Current Operating System
• Current Firewall
• Current Virus Protection
Media Storage and Access

- Media protection policy and procedures shall be documented and implemented to ensure that access to electronic media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

- The agency shall securely store electronic media within physically secure locations or controlled areas. The agency shall restrict access to electronic media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.
Electronic Media in Transit

- “Electronic media” means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

- Controls shall be in place to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in Section 5.10.1.2 of this Policy, is the optimal control during transport; however, if encryption of the data isn’t possible then each agency shall institute other controls to ensure the security of the data.
The agency shall protect and control electronic media and during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.
Use of Mobile Devices

- Laptop Devices
- Tablet Devices
- Pocket/Handheld Mobile Devices

Please refer to CJIS Security Policy

5.5.7.3.1
5.5.7.3.3
Compensating Controls for AA for Smartphones or Tablets

In the State of Texas

Please contact:

SecurityCommittee@dps.texas.gov
Okay, I'll be out of the office for two weeks. While I'm gone you will need my user id/ password-- don't worry we do it all the time.
Organizations shall, at a minimum, ensure that cellular devices:

- Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in section 5.10.4.1.
- Are configured for local device authentication.
- Use advanced authentication.
- Encrypt all CJI data resident on the device.
- Erase cached information when session is terminated.
- Employ personal firewalls or run a Mobile Device Management system that facilitates the ability to provide firewall services from the agency level.
- Employ antivirus software or run a Mobile Device Management system that facilitates the ability to provide antivirus services from the agency level.
5.5.7.3.3 Mobile Device Management (MDM)

Agencies shall implement the following controls when allowing CJI access from cell / smart phones and tablet devices that do not support Firewalls or Antivirus software.

MDM with centralized administration capable of at least:

- Remote locking of device
- Remote wiping of device
- Setting and locking device configuration
- Detection of “rooted” and / or “jailbroken” devices
- Enforce folder and / or disk level encryption
Electronic Storage

- Electronic storage of CHRI is allowed, unless retention of such information is not permitted by statute.

- All CHRI retained electronically in storage system must strictly follow FBI CJIS Security Policy 5.2.

- All CHRI must be contained in separate file folders within the system to prevent unauthorized access, use and dissemination of CHRI.
Electronic Media Sanitation and Disposal

- The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.
5.7.1.2 Network Diagram

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status.

The network topological drawing shall include the following:

- All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
- The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
- “For Official Use Only” (FOUO) markings.
- The agency name and date (day, month, and year) drawing was created or updated.
- Current Operating System
- Current Firewall
- Current Virus Protection
- Diagram (if the diagram cannot be released to the city/county agency, it may be sent to DPS directly)
- Agreements and possible fingerprints of contracted IT staff
- CJIS Security Training
Disabling Users

- Account supervisor(s) need to suspend a user’s account when a person no longer needs access to the secure site.
- Liability for the agency is potentially high if not done.
- Individual can still access criminal history from another location which would be a potential class B misdemeanor for unauthorized retrieval and purpose.
- Agency will be held liable for not disabling an individual’s access and all criminal history information retrieved by that individual.
Section §411.085 of the Texas Government Code

(a) A person commits an offense if the person knowingly or intentionally:

(1) obtains criminal history record information in an unauthorized manner;

uses the information for an unauthorized purpose,

or discloses the information to a person who is not entitled to the information;

(2) violates a rule of the department adopted under this subchapter.

(b) An offense under Subsection (a) is a Class B misdemeanor, except as provided by Subsection (c).

(c) An offense under Subsection (a) is a felony of the second degree if the person:

(1) obtains, uses, or discloses criminal history record information for remuneration or for the promise of remuneration; or

(2) employs another person to obtain, use, or disclose criminal history record information for remuneration or for the promise of remuneration.

(d) The department shall provide each person who applies for access to criminal history record information maintained by the department with a copy of this section.
Contact Information

- Non-Criminal Justice Audit and Training
  - (512) 424-7364
  - ncju@dps.texas.gov

- CJIS Security Office Team Lead
  - (512) 424-7876
  - Security.committee@dps.texas.gov