Proper Use of FBI Criminal Information

Policy

The Department of Children and Families (DCF) shall ensure the protection of FBI Criminal Justice Information (CJI) and its subset of FBI Criminal History Record Information (CHRI) until such time as the information is purged or destroyed in accordance with applicable record retention policies.

The following policies were developed using the FBI's Criminal Justice Information Services (CJIS) Security Policy. DCF may complement this policy with a local policy; however, the CJIS Security Policy shall always be the minimum standard. The local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

This policy shall apply to any electronic or physical media containing FBI CJI while being stored, accessed or physically moved from a secure location at DCF. In addition, this policy shall apply to any authorized person who accesses, stores or transports electronic or physical media.

Definitions

Authorized personnel mean an individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI data.

Criminal History Records Information (CHRI) means a subset of CJI and, for the purposes of this policy, is considered interchangeable. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI.

Legal reference: In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI.

Criminal Justice Information (CJI) means all of the FBI CJIS provided data necessary for DCF to perform its mandated functions including, but not limited to, biometric, identity history, biographic, property and case or incident history data.

Criminal Justice Information Services (CJIS) means the FBI database containing national criminal history information. CJIS can be access through the COLLECT terminal or the Live Scan device.

Electronic media means memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives or digital memory card.

Physical media means printed documents and imagery that contain CJI.

Physically secure location means a facility or office or an area, room or group of rooms within a facility or office with both the physical and personnel security controls sufficient to protect the FBI CJI and associated information systems.

Remote access means any temporary access to DCF's information system by a user (or an information system) communicating temporarily through an external, non-agency controlled network (*e.g.,* the internet).

Proper Access, Use and Dissemination of CHRI

Information obtained from the Interstate Identification Index (III) is considered CHRI. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing noncriminal justice administrative functions on behalf of the authorized recipient and the outsourcing of said functions has been approved by appropriate CJIS Systems Agency (CSA) or State Identification Bureau (SIB) officials with applicable agreements in place.

Legal reference: Rules governing the access, use and dissemination of CHRI are found in Title 28, Part 20, CFR.

Personnel Security Screening

Access to CJI and CHRI shall be restricted to authorized personnel.

DCF shall conduct a fingerprint-based background check for staff with direct access to CHRI for the purposes of licensing or employment within 30 days of employment or assignment, including those who have direct responsibility for configuring and maintaining DCF computer systems and networks with direct access to CJI, and any persons with access to physically secure locations or controlled areas containing CJI.

Security Awareness Training

Basic security awareness training shall be required within six months of initial employment or assignment, and biennially thereafter, for all personnel who have access to CJI.

Physical Security

The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls.

All physical access points into the agency's secure areas shall be authorized before granting access. DCF shall implement access controls and monitoring of physically secure areas for protecting all transmission and display mediums of CJI.

Only authorized personnel shall have access to physically secure non-public locations. DCF shall maintain and keep current a list of authorized personnel. Authorized personnel shall take necessary steps to prevent and protect the agency from physical, logical and electronic breaches.

Media Protection

Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored or actively being accessed.

DCF shall securely store electronic and physical media within physically secure locations or controlled areas. DCF shall restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted.

Media Transport

Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. DCF shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

Media Sanitization and Disposal

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs and other similar items used to process, store or transmit FBI CJI shall be properly disposed of in accordance with measures established by DCF.

Physical media (print-outs and other physical media) shall be disposed of by one of the following methods:

- shredding using DCF-issued shredders;
- placed in locked shredding bins for a private disposal company to come onsite and shred, witnessed by DCF personnel throughout the entire process; or
- incineration using DCF incinerators or witnessed by DCF personnel onsite at DCF or at a contractor incineration site, if conducted by non-authorized personnel.

Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier hard drives, etc.) shall be disposed of by one of the following methods:

- overwriting (at least 3 times) - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s or a combination of both) onto the location of the media where the file to be sanitized is located;
- degaussing - a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (*e.g.,* those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media; or
- destruction – a method of destroying magnetic media. As the name implies, destruction of magnetic media means to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

IT systems that have been used to process, store, or transmit FBI CJI or sensitive and classified information shall not be released from DCF's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

Account Management

DCF shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling and removing accounts. DCF shall validate information system accounts at least annually and shall document the validation process.

All accounts shall be reviewed at least annually by the designated CJIS point of contact (POC) or designee to ensure that access and account privileges commensurate with job functions, need-to-know, and employment status on systems that contain Criminal Justice Information. The POC may also conduct periodic reviews.

Remote Access

DCF shall authorize, monitor and control all methods of remote access to the information systems that can access, process, transmit or store FBI CJI.

DCF shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. DCF shall control all remote accesses through managed access control points. DCF may permit remote access for privileged functions only for compelling operational needs but shall document the rationale for such access in the security plan for the information system.

Utilizing publicly accessible computers to access, process, store or transmit CJI is prohibited. Publicly accessible computers include but are not limited to hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless DCF has established and documented the specific terms and conditions for personally owned information system usage.

A personal device includes any portable technology like cameras, USB flash drives, USB thumb drives, DVDs, CDs, air cards and mobile wireless devices such as Androids, Blackberry OS, Apple iOS, Windows Mobile, Symbian, tablets, laptops or any personal desktop computer. When bringing personal devices is authorized by DCF, they shall be controlled using the requirements of the CJIS Security Policy.

Reporting Information Security Events

DCF shall promptly report incident information to appropriate authorities to include the state Information Security Officer (ISO). Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, DCF shall employ automated mechanisms to assist in the reporting of security incidents.

All employees, contractors and third-party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of DCF assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

Policy Violation or Misuse Notification

Violation of any of the requirements contained in the CJIS Security Policy or Title 28, Part 20, CFR, by any authorized personnel may result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and/or termination of employment.

Likewise, violation of any of the requirements contained in the CJIS Security Policy or Title 28, Part 20, CFR, by any visitor may result in similar disciplinary action against the sponsoring employee and may also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.