



Oregon

John A. Kitzhaber, M.D., Governor

Department of State Police Law Enforcement Data System

P.O. Box 14360
Salem, OR 97309-5074
(503) 378-3055
FAX (503) 364-2661

July 17, 2012

Subject: Access Security for CJIS Physically Secure Locations

This information paper is provided in response to questions concerning which persons need to be fingerprinted based on their direct, physical, logical or remote access to criminal justice information (CJI), and how visitors are to be controlled or escorted at criminal justice information system (CJIS) physically secure locations.

The following information is from the FBI CJIS Security Policy, Version 5.1. Please refer to the definitions provided at the end of this paper for clarification, specifically on the definitions of direct access, physical access and access to CJI.

Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

Personnel Security Policy and Procedures

Minimum Screening Requirements for Individuals Requiring Access to CJI:

1. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI. However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS Criminal History Record Information (CHRI) IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with:

- (i) 5 CFR 731.106; and/or
- (ii) Office of Personnel Management policy, regulations, and guidance; and/or
- (iii) agency policy, regulations, and guidance.

Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

2. All requests for access shall be made as specified by the CJIS System Officer (CSO – LEADS Director). The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.

3. If a felony conviction of any kind exists, the hiring authority in the Interface Agency shall deny access to CJI. However, the hiring authority may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance. If a record of any other kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate. If the person

appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.

4. If the person is employed by a NCJA, the CSO or his/her designee, and, if applicable, the appropriate board maintaining management control, shall review the matter to determine if CJI access is appropriate. This same procedure applies if this person is found to be a fugitive or has an arrest history without conviction.

5. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI.

6. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.

7. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

Personnel Screening for Contractors and Vendors

In addition to meeting the requirements in paragraph 5.12.1.1, contractors and vendors shall meet the following requirements:

1. Prior to granting access to CJI, the Contracting Government Agency (CGA) on whose behalf the Contractor is retained shall verify identification via a state of residency and national fingerprint-based record check. However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances.

2. If a record of any kind is found, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the Contractor-appointed Security Officer.

3. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA or the CJA (if the CGA does not have the authority to view CHRI) shall review the matter. A Contractor employee found to have a criminal record consisting of felony conviction(s) shall be disqualified. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.

The CGA shall maintain a list of personnel who have been authorized access to CJI and shall, upon request, provide a current copy of the access list to the CSO.

Applicants with a record of misdemeanor offense(s) may be granted access if the CSO determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The CGA may request the CSO to review a denial of access determination.

Visitor Control

The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity. The agency shall maintain

visitor access records to the physically secure location (except for those areas officially designated as publicly accessible)

Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to electronic and physical 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 and physical media within physically secure locations or controlled areas. The agency 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 per section 5.10.1.2.

The following are excerpts from Oregon Administrative Rules:

The Oregon State Police (OSP) Criminal Justice Information Services (CJIS) Oregon Administrative Rule (OAR) 257-015-0050 User Responsibilities, Paragraph 6, Background Checks of Terminal Operators Required:

(6) "Background Checks of Terminal Operators Required" Policies for access to the FBI-NCIC system require background screening of all terminal operators with access to the NCIC system. For efficiency and consistency, the key elements of the NCIC background screening policies are also adopted for all LEDS access, as follows:

(a) Appropriate Background investigations, including a check of LEDS and NCIC fugitive warrant files, the Oregon computerized criminal history (CCH) system, and the FBI Interstate Identification Index (III), must be conducted on all terminal operators with LEDS access. To assure positive identification, submission of a completed applicant fingerprint card to the FBI Identification Division through the Oregon State Police Identification Services Section is also required;

(b) If the applicant is found to be a fugitive or to be the subject of a current prosecution, access will be denied. If the applicant has been convicted of a crime which could have resulted in a sentence to a Federal or State penitentiary, access will be denied;

(c) Exceptions to denials based upon prior criminal convictions may be made in extraordinary circumstances upon application by the user agency to the Superintendent of State Police setting forth the circumstances. The Superintendent or his/her designee will maintain a central file where such exception authorizations shall be filed.

The Oregon State Police (OSP) Identification Services Section, Oregon Administrative Rule (OAR) 257-010-0025 Access to and Use of Criminal Offender Information, Paragraphs 4 and 5:

(4) Criminal offender information may be furnished to authorized Criminal Justice and Designated Agency employees and no person who has been convicted of a crime which could have resulted in a sentence to a federal or state penitentiary will be allowed to operate a computer terminal accessing CCH information or have access to Criminal offender information. All authorized agency employees as described above must be fingerprinted and the fingerprint card submitted to OSP. The fingerprint cards will be searched against the state and federal criminal record files. The "Reason Fingerprinted" may be for criminal justice employment such as "Police Officer," "Corrections Officer" or "Access to CCH (or CJIS Security)." These fingerprint cards will be retained by OSP and entered into the CCH File. Exceptions to this rule may be made in extraordinary circumstances upon written application to the Superintendent of the Oregon State Police setting forth such circumstances. The Superintendent of OSP will maintain a central file where such exception authorization shall be filed.

(5) Screening of Criminal Justice and Designated Agency employees who have access to CCH or criminal offender information records is the responsibility of the employing agency.

Based on the above sources, beyond that which is clear in the text provided, and because these questions continue to come up, LEDS makes the following interpretation of above sources, which is not all inclusive (i.e. see above).

The following persons must undergo a fingerprint-based background check:

- a. **Persons who directly access CJI by any mode.**
- b. **Persons/vendors who configure and maintain computer systems and networks with direct access to FBI CJIS systems.**
- c. **Any person, with unescorted access to CJIS physically secure locations (terminal areas) regardless of the status of the terminal.**
- d. **Any person with unescorted access to areas where CJI or CHRI printouts are openly stored within the physically secure location.**
- e. **Any person who by virtue of their duties receives an electronic or paper copy of CHRI, excluding elected officials at criminal justice agencies and Oregon Circuit Court judges.**

One bottom line interpretation from these definitions is if a person/visitor has the physical ability to view CJI while in your agency and they are unescorted, they have access to CJI and must be fingerprinted. If they are escorted, then you must take necessary steps to ensure CJI will not be compromised.

Relevant Definitions from the FBI CJIS Security Policy Version 5.1

Access to Criminal Justice Information — The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

Authorized User/Personnel — 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 Justice Information (CJI) — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property, and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions.

Criminal History Record Information (CHRI) — A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Direct Access — (1) Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, Part 20). (2) Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

Escort – Authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

Physical Access – The physical ability, right or privilege to view, modify or make use of Criminal Justice Information (CJI) by means of physical presence within the proximity of computers and

network devices (e.g. the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

Physically Secure Location — A facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. For interim compliance, a police vehicle shall be considered a physically secure location until September 30th, 2013. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods, with section 5.9.1.3.

For questions on this topic, please contact the LEDS Auditor, Dan Malin at 503-378-3055, extension 55007 or email to dan.malin@state.or.us.