LEDS FREQUENTLY ASKED QUESTIONS

Question: ***What is the warrant entry timeline? Some say NCIC gives agencies 24 hours, others say NCIC gives up to seven days.***

Answer: The following excerpt from the NCIC 2000 Operating Manual Chapter on Wanted Persons is clear:

1.1 CRITERIA FOR ENTRY

1. GENERAL CRITERIA

An entry in the Wanted Person File should be made immediately after:

1) the decision to arrest or authorize arrest has been made, **and**

2) the decision has been made regarding extradition.

The following question came from a LEDS Representative.

Question: ***I am attempting to enter the SID number into the LEDS Training Record for my agency's employees and am getting a reject message. How can I resolve this so I can enter the SID numbers?***

Answer: LEDS is set up so that you can only enter the SID number for those employees who underwent a fingerprint based background check for CJIS Security (8804) with your agency's ORI on the fingerprint card. Ensure all new employees or reprints are printed with the CJIS Security purpose written on the fingerprint card with your agency ORI.

Question: ***Does my agency's shredding service meet CJIS security policy requirements?***

If LEDS/CCH records are included in the shred bins and the bins are escorted to the shredding truck by a LEDS cleared (printed) person, and the shredding is done at the curbside, your agency meets the requirements.

If your LEDS/CCH records are placed in a bin, box or bag, and those records leave your CJIS secure area to be shredded elsewhere, then the persons who provide that shredding service, including the driver and anyone who works at the shredding facility must undergo a fingerprint-based background check for CJIS security.

Reference: NCIC CJIS Security Policy, Section 4.5.1.(a)
OAR 257-010-0025 (4)

The following question has been asked by several LEDS Representatives concerning validations.

Question: ***In the event of accidental destruction of records due to fire, flood or accidental shredding, or in the case where the victim is deceased or otherwise no longer available, how can the record be maintained in LEDS or NCIC and validated, when the supporting case file, documentation, or victim is not available?***

NCIC's validation policy states "Validation is accomplished by reviewing the original entry and current supporting documents, and by recent consultation with any appropriate complainant, victim, prosecutor, court, non-terminal agency, or other appropriate source or individual. In the event the ORI is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority must make a determination based on the best information and knowledge available whether or not to retain the entry in the file."

This leaves the decision up to the entering agency, and generally we would encourage agencies to remove the record, but caution is urged concerning those records that could affect officer safety, such as guns. If the agency decides to leave the record in LEDS and NCIC, then a memorandum for the record should be prepared stating that while the supporting documentation or victim are no longer available for record validation purposes, out of concern for officer safety, this agency has determined that leaving this record in LEDS/NCIC is in the best interest of public safety.

Question: ***Where can I find the legal basis for required fingerprint based background checks?***

We receive many questions concerning who must be fingerprinted for access to CJIS systems and information, and the following information is provided.

A CJIS secure area is any area where CJIS data, CJIS network equipment, or CJIS systems are located, used, stored, or accessed.

For access to CJIS secure areas, who needs to be fingerprinted?

1. Anyone who operates a terminal (PC, laptop, MDT, hand held device) that may be used to access LEDS or NCIC data.

Responsible Agency: OSP CJIS

Point of Contact: Dan Malin, CJIS Auditor,
dan.malin@state.or.us
503-378-3055, ext. 55007

Reference: OAR 257-015-0050 User Responsibilities:

(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;"

2. Anyone with access to Oregon criminal history information (either by operating a terminal or receiving the information from someone else).

Responsible Agency: OSP Identification Services Section

Point of Contact: Kathy Cea, CCH Records Unit Manager,
Kathy.cea@state.or.us
503-378-3070

Reference: OAR 257-010-0025 Access to and Use of Criminal Offender Information:

"(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." 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."

3. Anyone who has unescorted access to a CJIS secure area.

Responsible Agency: FBI CJIS

Point of Contact: Michael Curtis, OSP CJIS Information Security Officer,
michael.curtis@state.or.us
503-378-3055, ext. 55004

Reference: FBI CJIS Security Policy Version 4.4, Chapter 4 – Security Enforcement

4.0 SECURITY ENFORCEMENT

4.4 Physical Security

4.4.1 Computer Facility Security: The computer site and related infrastructures (e.g., information system servers, controlled interface equipment, associated peripherals, communications equipment, wire closets, patch panels, etc., including police vehicles if they house equipment which provides access to the CJIS network) must have adequate physical security at all times to protect against any unauthorized access to or routine viewing of computer devices, access devices, and printed and stored data.

4.4.3 Visitors Access: All visitors to computer centers and/or terminal areas (CJIS secure areas) shall be escorted by authorized personnel at all times.

4.5 Personnel Security

4.5.1 Personnel Background Screening for Systems Access and Computer Terminal/ Records Storage Areas Access

a) To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days upon initial employment or assignment for all personnel who have authorized access to FBI CJIS systems and those who have direct responsibility to configure and maintain computer systems and networks with direct access to FBI CJIS systems. Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint based record check. All requests for systems access shall be made as specified by the CSO. The CSO, or their official designee, is authorized to approve CJIS systems access. All official designees to the CSO shall be from an authorized criminal justice agency.

NCIC's definition of Authorized Access:

Authorized Access - the ability to perform an authorized transaction from a CJIS terminal device <u>or having access to CJIS data</u> that is routinely prohibited by organizational policy or law by satisfying the appropriate background checks, clearance and training.