Oregon
Theodore R. Kulongoski, Governor

Department of State Police
Law Enforcement Data System
P.O. Box 14360
Salem, OR 97309-5074
(503) 378-3055
FAX (503) 364-2661

To Agency LEDS Representatives

Subject: 2005 FBI Audit Results

This document contains vital training information pertaining to the 2005 Oregon FBI NCIC audit cycle. We are providing this information to aid in the training and education of your staff.

Although this document discusses both broad areas of concern and deficiencies that must be addressed, we fully recognize the 2003 elimination of both the LEDS Training and Audit units have a direct correlation with, and impact on, the findings of this audit. Furthermore, the hallmark of LEDS has always been that of superior customer service; over the next twelve months we will be working closely with our various constituencies to refine existing training tools & guidelines and our audit policies and procedures. In addition, we will be looking for more efficient ways we can provide the highest possible customer service.

This document is organized in the in the following manner:

The main body of this document contains summary information on areas of concern.
Appendix "A" – Policies and procedures for submitting applicant fingerprint cards for people accessing LEDS/NCIC.
Appendix "B" – Oregon Administrative Rules.

MAIN BODY

The following pages highlight areas of non-compliance and/or significant concern to LEDS and the FBI. Please make this information available to all applicable personnel. Furthermore, please review, in detail with your staff, all policies and procedures applicable to your career discipline to ensure your agency is in compliance.

It is critical that all possible measures be taken to further reduce error rates and correct areas of non-compliance with NCIC policy; in doing so, we will lower or completely mitigate areas of potential liability, increase the apprehension rate of criminals and the recovery of stolen property, and decrease the potential for injury or death to criminal justice employees and the citizens of the state of Oregon. Should you have any questions, please contact me via email at robert.b.morris@state.or.us.

BACKGROUND INFORMATION

The FBI CJIS audit staff conducted its tenth biennial NCIC audit of LEDS and Oregon agencies in November and December 2005. The FBI is mandated to audit every federal and state CJIS Systems Agency (CSA) every three years to ensure the integrity of data maintained in criminal justice systems managed by the FBI. LEDS is the CSA for the state of Oregon. Analysts who conduct on-site audits at LEDS and on-site reviews at Oregon agencies assess the integrity of data maintained in these databases. Policies and procedures outlined in Oregon Revised Statutes, Oregon Administrative Rules, and the LEDS Operating and LEDS Rep. Manuals are examined during this process.

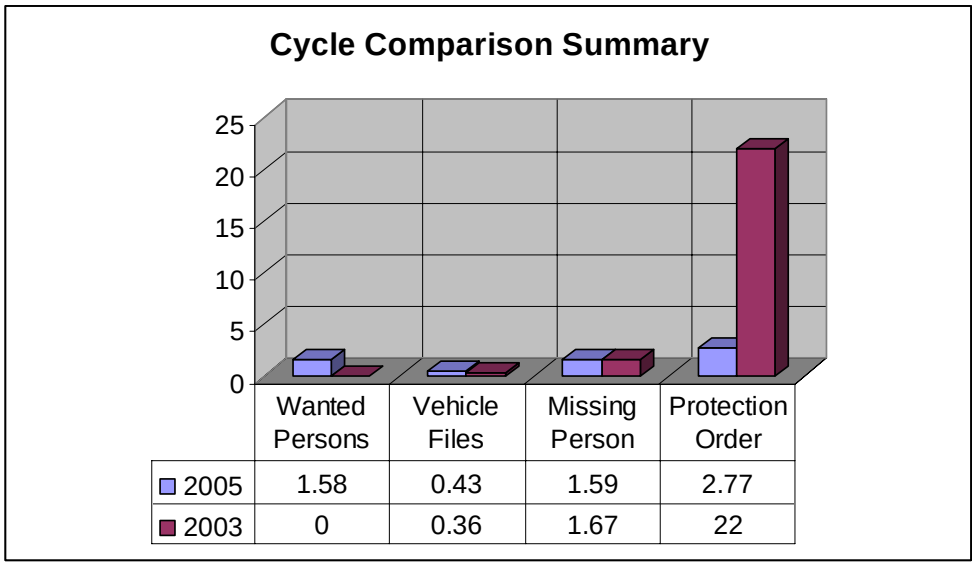
The local agency phase of NCIC audits includes three components:

- Policy compliance review;
- Data quality check of the Wanted Person, Vehicle, Missing Person, and Protection Order Files;
- A risk analysis of the agency's record maintenance procedures.

The local review gathers information on policy compliance related to record maintenance, III, and system security. Additionally, data is collected on NCIC operator training, response times, timely entry and removal of records, and data quality. The data quality check verifies the record's validity, accuracy, and completeness. Information compiled during the local agency policy review and data quality check is used to formulate a risk analysis. The risk analysis identifies areas that should be improved by local agency management to establish more effective controls over its LEDS and NCIC record maintenance process.

The FBI auditors review record entries into LEDS and NCIC to document the timeliness of entries. Timely entry of records is essential to ensure system effectiveness and provides maximum protection to the law enforcement officer by providing up-to-date information. Delayed entry of record reduces or completely eliminates the possibility of apprehending wanted persons, recovering stolen property, and providing pertinent information in locating missing persons. Equally important is the timely removal of invalid records from the system; failure to ensure records are promptly removed as soon as the record becomes invalid places the agency at a greater risk for civil litigation as well as increases the risk to officers and citizens alike.

The following chart depicts and compares the composite error rates identified in both the 2003 and 2005 audit cycle. During the next audit cycle, the convicted Sexual Offender Registry File will be added to the files examined and will be subject to the same sanctions as the other files.



AUDITING / TECHNICAL 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 LEDS/NCIC) must have adequate security at all time to protect against any unauthorized access to, or routine viewing of, computer devices, access devises, and printer and stored data.

PASSWORDS: Agencies permitting LEDS/NCIC access via a network, must establish authentication of users by a user ID and a unique password combination. Passwords must with the following secure attributes:

1) Passwords shall:
   a) Be at minimum length of eight (8) characters on systems procured after 09/30/05
      i) and on ALL systems by 09/30/2010.
   b) Not be a dictionary word or proper name
   c) Be different than the user name
   d) Be changed within a maximum of every 90 days
   e) Not be transmitted in the clear outside the secure domain

Note: On systems obtained after 09/30/05 shall prevent password reuse of the last ten (10) passwords.

WIRELESS DATA ENCRYPTION: All wireless upgrades after 09/30/2002 shall support a minimum of 128-bit encryption for all data. Any procurement for wireless devices after 09/30/2005 shall require a minimum of 128-bit encryption with NIST, CSL certification of the cryptographic module to ensure it meets FIPS Publication 140-2 for "Security Requirements for Cryptographic modules." Any wireless device with a required minimum of 128-bit encryption BEFORE 09/30/2005 does NOT require NIST, CSL certification UNTIL 09/30/2010.

PUBLIC NETWORK SEGMENT SECURITY: A "public network" segment for CJIS purposes is defined as a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by a criminal justice agency, i.e., telecommunications infrastructure which supports a variety of users other than criminal justice or law enforcement. Examples of public networks/segments include, but are not limited to; dial-up and Internet connections, ATM frame relay clouds, wireless networks, wireless links, and cellular telephones.

All CJIS data transmitted through any public network segment or over dial-up or Internet connections (does not include radio frequency transmissions) shall be immediately protected of with a minimum 128-bit encryption. This requirement also applies to any private data circuit that is shared with non-criminal justice users and/or is under the direct management control or a criminal justice agency.

SECURITY AUDITS: The CJIS Security Policy states the CSA shall conduct security audits for operational systems at least once every three (3) years to ensure all interface agencies shall establish an audit trail capable of monitoring successful and unsuccessful log-on attempts, file access, type of transaction and password changes. Due to budget constraints and limitations, to date, LEDS has not been sufficiently staffed to meet this mandate. Over the next months LEDS will be working to correct this deficiency.

ADMINISTRATIVE AUDITS: Further, FBI Policy requires we conduct audits of all terminal agencies at least once every three years. Due to the elimination of the Audit and Training Units in 2003, we were unable to satisfy this mandate. We recognize our inability to meet this requirement has contributed, in part, to some of the deficiencies noted in theses most recent audit results. Again, we are working to correct this deficiency by attempting to secure a stable funding source for both of these vital programs.

TERMINAL AND PERSONNEL SECURITY

The FBI CJIS Security Policy requires state and national fingerprint-based check must be conducted within 30 days of initial employment or assignment for all personnel, including appropriate information technology (IT) personnel, that have access to the CJIS systems. Furthermore, agencies must screen custodial, support, and/or contractor personnel through established personnel background screening methods, ***unless escorted at all times***, by authorized personnel. At minimum, such personnel must submit to a fingerprint based background check.

Per LEDS policy, prior to allowing anyone access to LEDS/CJIS secure areas, the agency LEDS Representative will ensure an automated CCH check has been conducted on such person(s). If the person has been convicted of any crime punishable by imprisonment for greater than one year, access will be denied; if the agency feels an exemption of this exclusion is warranted due to mitigating circumstances, the agency may apply to LEDS for relief from this exclusion on a case by case basis.

If the person is free from any such convictions, access may be immediately grated on a temporary basis pending definitive confirmation via submission of fingerprints. When submitting applicant fingerprint cards for the purpose of satisfying this mandate, the “reason printed” box must contain the code “8804 – CJIS Security”. This code creates a “flag” in the system that, in the event such employee is arrested, the system will automatically generate a notification message to LEDS that the person has been arrested. LEDS will then notify the employing agency of such action.

Appendix of “A” of this packet contains the Oregon State Police Identification Services Section procedures and forms necessary to process an applicant fingerprint card pursuant to this policy.

CCH CONFIDENTIALITY:

The FBI determined that some agencies were out of compliance. Non-compliance was determined through an administrative interview with the local agency personnel and through the results of the III survey form. Authorization to obtain records via the Interstate Identification Index (III) is governed by federal laws and state statutes approved by the U.S. Attorney General.

Operators shall use the terminal only for those purposes, which are authorized. Copies of III data obtained from terminal devices must be afforded security to prevent any unauthorized access to, or use of, the data.

III records shall be maintained in a secure records environment. Such storage of records may be for extended periods ONLY when the III records are key elements for the integrity/utility of the case files/criminal record files in which they are retained. When retention of III records is no longer required, final destruction shall be accomplished in a secure manner so as to preclude unauthorized access/use.

CCH AND OTHER SENSITIVE RECORD DESTRUCTION:

III records should be properly destroyed when the record is no longer current by authorized and backgrounded agency personnel. The CJIS Security Policy states, in-part, that private contractors shall be permitted access to CJIS record information systems pursuant to an agreement which specifies the contactor's purpose and scope of providing services for the administration of criminal justice; [i.e. shredding of III and other LEDS/NCIC documents.] The agreement between the criminal justice government agency and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI (acting for the US Attorney General) as referenced in the Title 28 CFR 20.33 (a)(7). Private contractors who perform the administration of criminal justice shall meet the same training and certification criteria required by governmental agencies performing a similar function and shall be subject to the same extent of audit review as are local users.

All private contractors who have been permitted to access the CJIS record information systems shall abide by all aspects of the CJIS Security Addendum. Modification to the CJIS Security Addendum shall be enacted only by the FBI.

GENERAL USE GUIDELINES:

Computerized criminal history records are available to criminal justice, and authorized non-criminal agencies via LEDS from the Oregon State Police Identification Services Section Criminal History Files and from the NCIC Interstate Identification Index (III). All agencies accessing these files must have an agreement, signed by the current agency administrator, with LEDS and must adhere to Administrative Rules (Chapter 257-015-0000 through 257-015-0100) adopted by the Department of State Police. Because additions or deletions may be made at any time, a new copy should be requested when needed for subsequent use. Agencies accessing CCH information must strictly adhere to the policies and purpose codes governing access.

Section 257-015-060 of the LEDS Administrative Rules, states, in part:

> Information is made available to LEDS users from various sources and agencies, including LEDS and other state information system files, motor vehicle departments, NCIC, Oregon State Police Identification Services Section, etc. Each user must observe any restrictions placed on the use or dissemination of information by its source. It is LEDS' responsibility to advise user agencies of any restrictions which apply to any information accessed via the Law Enforcement Data System.
>
> (1) Investigative Files: Information from investigative files maintained by LEDS, NCIC, or other agencies is for criminal justice use only and is not to be disseminated to any person for other than an official criminal justice purpose. Inquiries from the public regarding the status of an investigative file should be referred to the agency holding the case.
>
> (2) Oregon Computerized Criminal History Records (CCH):
>
> (a) Oregon criminal history records are available via LEDS, from the Oregon State Police Computerized Criminal History Files, to agencies which are authorized by the Oregon State Police.
>
> (b) All agencies accessing the Oregon CCH files must have a signed agreement with the Oregon State Police and must adhere to Oregon Administrative Rules (OAR) 257-010-0025 through 257-010-0050 adopted by the Department of State Police.
>
> (3) Federal Bureau of Investigation - Interstate Identification Index (FBI-III): The Federal Bureau of Investigation maintains the Interstate Criminal Identification Index which is available through LEDS. Access to this information is restricted to criminal justice agencies, as defined in OAR 257-015-0015(5), in the discharge of their official responsibilities, or to non-criminal justice agencies which provide services to criminal justice agencies, and which have signed a management control agreement with a criminal justice agency.

All information contained in Oregon criminal history records falls within the provision established by the Oregon Public Records Law as outlined in the Oregon Revised Statutes. Individuals wanting copies of Oregon CCH records pertaining to **anyone**, other than themselves, may obtain copies of such records by contacting the Identification Services Section of the Oregon State Police. There is a fee for these records and the person that is the subject of the record **will be notified**, if a CCH exists. However, the person cannot prevent the release of such record; they may, at most, delay the release of the record for a period of time that is no greater than that required to validate the information contained in the record.

Inquiries for review or challenge of records are strictly prohibited. If an individual wishes to review, challenge, or has questions about ***their own record*** they must contact the Identification Services Section of the Oregon State Police, as set forth in the provisions of Oregon Administrative Rules, Chapter 257. ***NO ONE*** except criminal justice personnel, or other persons designated by law, who are acting in their official capacity, for ***AN AUTHORIZED PURPOSE***, may view criminal history records. This rule does not apply to criminal justice personnel when running ***THEIR OWN*** criminal history for the purpose of LEDS Training.

CCH PURPOSE CODES:

C	Criminal Justice	Used for official duties in connection with the administration of criminal justice.
J	Criminal Justice Employment	Used when the III transaction involves employment with a criminal justice agency or the screening of employees of other agencies over which the criminal justice agency maintains management control. Criminal justice employment has been separated from other criminal justice purposes due to the requirement of some state agencies participating in III. For those states that are unable to provide a record for a purpose code J inquiry (i.e. state statute), the FBI will provide the record on-line.
F	Weapons Related Checks	Used when the III transaction involves weapons-related background checks authorized by the state. All firearm-related checks must be made through the National Instant Criminal Background Check System
D	Domestic Violence and Stalking	Used by civil or criminal courts in domestic violence or stalking cases. ORI's ending in D, A, I, OR J.
H	Housing	Used when the III inquiry is made under the authority of the Housing Opportunity Extension Act of 1996. Limited to QH inquiries.
A	Administrative File Maintenance	Used when the authorized participating state agency generates a III for internal review. Responses for this purpose code may not be disseminated for any other reason. Responses are limited to that state's portion of the record maintained by the FBI. No federal arrest data are reported.
S	National Security	Used when the III transaction is generated by an agency authorized by the Security Clearance Information Act (SCIA) in investigation of individuals for access to classified information or assignment in sensitive national security duties. Limited to an ORI not starting with OR0, ORD0A, ORDI, ORSP or ORVA.
V	Visa Applicants	Used when the III transaction is made for the purpose of determining eligibility for visa application. Limited to QH inquiries by the Department of State, Consolidated Immigrant Processing Visa Center. (Any Oregon ORI beginning with ORINS or any out-of-state ORI)
E	Non-Criminal Justice Agency Employment	This code is to be used when an inquiry is being made by a criminal justice agency into the background of an individual who has applied to be an employee or agent of a non-criminal justice agency. Examples are: Employees, contractors, volunteers, block-home parents, foster parents, etc. Such an inquiry may be made only when the criminal justice agency has written policy documenting its specific legal and official responsibility for such background investigations. **Purpose code "E" is valid for Oregon CCH inquiries only.** Information in a criminal record may not be shared with the non-criminal justice agency. Typically, the criminal justice agency will recommend approval or denial, based upon the criminal record check and other elements of the background investigation. Depending upon the circumstances, the criminal justice agency may refer the non-criminal justice agency to the Oregon State Police Identification Services Section, in Salem, where the public criminal history record may be obtained for a fee.
L	Licensing	This code is to be used when an inquiry is being made into the background of a license or permit applicant. Examples are: Foster care provider background checks, OLCC licensing, card room licensing, taxi licenses, explosives licenses, etc. Such an inquiry may be made only when there exists a specific state or federal statute or local ordinance requiring an investigation into past criminal conduct as a condition of obtaining the license or permit. **Purpose code "L" is valid for Oregon CCH inquiries only.**
X	Emergency placement of children in exigent circumstances	Used by specific agencies to determine the fitness of a person to assume temporary custody of a child(ren) in an emergency situation where sufficient time is not available to process the applicant through normal channels. Limited to any ORI Ending in "T"

ADMINISTRATIVE ISSUES

The primary responsibility for the entry and maintenance of accurate, timely, and complete records lies with the entering agency. However, LEDS assumes a large degree of administrative responsibility to ensure this mandate is being satisfied. Criminal justice agencies specifically have a legal duty to maintain records that are accurate, complete, and up-to-date. The following standards have been established and approved by the CJIS Advisory Policy Board (APB):

ACCURACY/COMPLETENESS:

Entries must contain only correct data. Complete records include all information available at the time of entry. Record validation must also include a comprehensive attempt to obtain any and all additional information for which there is a corresponding field in the LEDS and/or NCIC system.

Such information includes, but is not limited to:

- Caution indicators
- AKA Names
- AKA DOBs
- Scars, Marks, Tattoos, Medical Conditions, Piercings
- Social Security Numbers,
- Operators' License Numbers,
- Vehicle License Numbers

TIMELINESS OF RECORD ENTRY:

Any agency having investigative authority and jurisdiction must enter records into LEDS and NCIC that meet the specified entry criteria. Appropriate entry of data and records into the system, unless otherwise noted, must be made as soon as possible after the receipt of validated crime or incident report. This timeliness policy pertains to ALL records maintained in LEDS and/or NCIC. Examples of files include, but are not limited to, Wanted Person, Missing Persons, Protection Orders, Articles, Boat, Guns, etc.

MISSING PERSON RECORDS: Specifically pertaining to the missing person file, a record of a

1) Missing Adult; person over the age of 21:
   a) Should be entered as soon as possible after the entering agency has signed documentation supporting the stated conditions under which the person is declared missing, but in no case shall the delay exceed twelve (12) hours. This written documentation will aid in the protection of the individual's right to privacy.

      i) In the absence of documentation from a parent, legal guardian, next of kin, physician, or other authoritative source, including a friend or neighbor in unusual circumstances, or when such documentation is not reasonably attainable, a signed report by the investigating officer will suffice.

2) Missing Child; person under the age of 21:
   a) The National Child Search Assistance Act (42 USC § 5779 and 5780) forbids all law enforcement agencies in the country from establishing any waiting period before accepting a missing child report. In addition, the act requires the IMMEDIATE entry of each report into the National Crime Information Center (NCIC) computer and DOES NOT limit the instigation of a missing child report, or investigation, to the custodial parent.

      i) For record entry purposes under this act, a child is defined as anyone under the age of 21.

   b) According to the FBI's Child Abduction and Serial Murder Investigative Resources Center (CASMIRC), the first 48 hours after an abduction is the most critical to the safe recovery of the child. For this reason NCIC created a special missing person record type code, which, when entered into a missing person record, enables NCIC to automatically notify the CASMIRC and the National Center for Missing and Exploited Children. Technical and investigative assistance can then be provided to the investigating agency. To facilitate this notification, whenever a child may have been abducted and their life may be in danger, regardless if it was a stranger abduction or a family abduction YOU MUST CHANGE THE "MNP" CODE TO "CA" WHICH STANDS FOR "CHILD ABDUCTION".

   c) Pursuant to the National Child Search Assistance Act of 1990, no later than 60 days after the original entry of the record into the state law enforcement system and NCIC computer networks, all law enforcement agencies are required to verify and update such records with any and all additional information, including medical and dental record information. (Title 42, U.S.C., Chapter 72, Section 5780)

SECOND PARTY CHECKS:

The accuracy of the LEDS and NCIC records is an integral part of the system. The accuracy of a record ***MUST*** be double-checked by a second party. The verification of a record should include assuring all available cross checks, e.g. VIN/LIC, NAME, DOB, OLN, OLS, SOC, etc. are made and that the data in the record match the data in the investigative report.

Agencies lacking staff support for this verification should require the case officer to check the accuracy of the record, as the case officer carries the primary responsibility for seeking the fugitive or recovering the stolen property.

VALIDATION:

Validation is accomplished by reviewing the original entry and current supporting documents, and by recent consultation with any appropriate complainant, victim, prosecutor, court, or other appropriate source or individual. In the event the agency 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 original entry in the file.

It should be noted the validation of records was cited as a recommendation in the 2003 audit, but continues to be a concern throughout this audit cycle.

Once the validation process is completed, the LEDS Rep is required to return the validation certification form, affirming all records contained on that listing have been properly validated, to LEDS on or before the due date. All records must contain clearly identified extradition limits, and hit confirmation information, including a current telephone number that is staffed 24 hours a day.

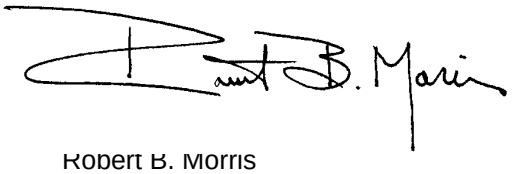
The 2006 LEDS Workshop will be held September 11th, 12th, 13th, & 14th in Seaside, at the Convention Center. Detailed information on these topics, and others, will be presented.

Our workshops as well as any other training we sponsor is open to ANYONE who wishes to attend, unless otherwise stated in the training announcement. There are currently more than 14,000 active LEDS certified personnel in the state of Oregon, and although the majority of the attendees of the annual workshop are LEDS Reps., the training is NOT restricted to LEDS Reps.

Because the information presented at the workshop is applicable to all LEDS users, we encourage anyone interested in attending to make their interest known to their supervisor.

On behalf of LEDS, thank you for your continued support! Our shared goal of excellence could not accomplished without your commitment and diligence.

Sincerely,



Robert B. Morris
Training & Education Manager

APPENDIX "A"

Policies and procedures for submitting applicant fingerprint cards for people accessing LEDS/NCIC.

APPENDIX "B"

Oregon Administrative Rules

The Oregon Administrative Rules contain OARs filed through March 15, 2006

DEPARTMENT OF OREGON STATE POLICE

DIVISION 15
LAW ENFORCEMENT DATA SYSTEM (LEDS)

[**ED. NOTE**: Chapter 188, Oregon Laws 1993 transferred rulemaking authority from the Criminal Justice Services Division, Executive Department, OAR Chapter 107 to Department of State Police, OAR Chapter 257.]

257-015-0000
Purpose of Rules
Rules adopted herein prescribe the policies and procedures for operation and use of the Oregon Law Enforcement Data System (LEDS).
Stat. Auth.: ORS 181.730(3)
Stats. Implemented: ORS 181.730
Hist.: OSP 1-1995, f. & cert. ef. 8-15-95

257-015-0010
Authority
(1) The Law Enforcement Data System (LEDS) was established by act of the 1969 Oregon Legislature (ORS 181.710) which authorized the state Executive Department to develop and operate a police information network. In 1973, the term "Police Information Network" was amended to read "Law Enforcement Data System". Senate Bill 1044 in the 1993 legislative session transferred LEDS to the Department of Oregon State Police (ORS 181.730).
(2) The Law Enforcement Data System is a program organized within the Intergovernmental Services Bureau of the Department of Oregon State Police. It provides a criminal justice telecommunications and information system for the State of Oregon, and is the control point for access to similar programs operated by other states and the Federal Government.
Stat. Auth.: ORS 181.730(3)
Stats. Implemented: ORS 181.730
Hist.: OSP 1-1995, f. & cert. ef. 8-15-95

257-015-0020
Law Enforcement Data System (LEDS) Advisory Committee
(1) The LEDS Advisory Committee advises the Superintendent of State Police on general policy concerning the philosophy, concept, and operational principles of the LEDS program. In its deliberations the Committee places particular emphasis on the following areas:
(a) Continued responsiveness of the LEDS program to the state's criminal justice information needs;
(b) System security; and
(c) Rules, regulations and procedures to maintain the integrity of LEDS information.
(2) The LEDS Advisory Committee is composed of members appointed by the Governor representing the following areas:
(a) The Judicial Department;
(b) The Oregon Juvenile Department Directors' Association;
(c) The Oregon Peace Officers' Association;
(d) The Associated Public Safety Communications Officers, Inc.;
(e) The Oregon Association of Chiefs of Police;
(f) The Oregon State Sheriffs' Association;
(g) The Oregon District Attorneys' Association;
(h) Attorney General;
(i) The Oregon State Police;
(j) The Department of Transportation, Driver and Motor Vehicle Services Branch (DMV);
(k) The Department of Corrections;
(l) The Oregon Youth Authority; and
(m) Such other members as the Governor considers appropriate for purposes of the committee.
Stat. Auth.: ORS 181.730(3)
Stats. Implemented: ORS 181.730
Hist.: OSP 1-1995, f. & cert. ef. 8-15-95; OSP 2-1998, f. & cert. ef. 10-6-98

257-015-0030
Definitions
(1) "LEDS" means the Department of State Police, Law Enforcement Data System.
(2) "NCIC" means the Federal Bureau of Investigation, National Crime Information Center.
(3) "NLETS" means the National Law Enforcement Telecommunications System, Incorporated.
(4) "Associated Systems" means any automated or manual information system, which is accessible via LEDS.
(5) "Criminal Justice Agency" means the following as defined by the National Crime Information Center:
(a) Courts;

(b) A government agency or any subunit thereof which performs the administration of criminal justice pursuant to a statute or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice.
(6) "Criminal Justice Purpose" means: The administration of criminal justice, as defined in section (7) of this rule.
(7) The "Administration of Criminal Justice" means performance of any of the following activities: detection, apprehension, detention, pretrial release, post trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history record information. Criminal justice employment investigations are included, as is the licensing of or issuing of a permit for a weapon or explosive when required to be performed by a criminal justice agency, pursuant to a federal, state or local law. (This category includes firearms dealers and purchasers, carriers of concealed weapons, explosives dealers and users and lethal weapons dealers and users). State and Federal Inspector General offices are included. Defense of accused persons, whether by private counsel, public defender or other court appointed counsel is not included in the definition of the administration of criminal justice.
(8) "Investigative Files" means computerized records stored in LEDS, NCIC or other state criminal justice information systems, as follows: outstanding arrest warrants and other wanted persons; missing persons; unidentified persons; restraining orders; lost or stolen identification; Psychiatric Security Review Board Orders; persons who have threatened a Secret Service protected person; Persons under the supervision of a Court or a Corrections agency; gang members; armed career criminals; Sex offender registrants; concealed handgun license records; stolen, repossessed, impounded vehicles; stolen vehicle license plates, vehicle parts, vehicle identification plates and title certificates; vehicles used in the commission of a felony; stolen and pawned firearms; stolen securities; stolen boats and associated equipment; other stolen and pawned property; other files of a similar nature which may be established to assist in law enforcement investigations or to enhance other criminal justice purposes.
(9) "NCIC State Control Terminal Agency" means the agency in each state which is responsible for the state's computer link with the National Crime Information Center and which is responsible for ensuring that NCIC system security and operational policies and procedures are carried out within the state.
(10) "NLETS State Control Terminal Agency" means the agency in each state which is responsible for the state's computer link with the National Law Enforcement Telecommunications System, Inc., and which is responsible for ensuring that NLETS' system security and operational policies and procedures are carried out within the state.
(11) "Management Control Agreement" means a written agreement between a criminal justice agency and a non-criminal justice agency, which provides services (dispatching, record keeping, computer services, etc.) to the criminal justice agency. The agreement gives the criminal justice agency management control over the operations of the non-criminal justice agency as they relate to access to the Law Enforcement Data System network.
(12) "Management Control" means the authority to set and enforce:
(a) Priorities;
(b) Standards for the selection, supervision and termination of personnel; and
(c) Policy governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit information to or receive information from the Law Enforcement Data System.
Stat. Auth.: ORS 181.730(3)
Stats. Implemented: ORS 181.730
Hist.: OSP 1-1995, f. & cert. ef. 8-15-95; OSP 2-1998, f. & cert. ef. 10-6-98

257-015-0040
LEDS Responsibilities
The general responsibilities of the Law Enforcement Data System program are as follows:
(1) Develop and operate a computerized criminal justice telecommunications and information system providing message switching and record storage and retrieval capabilities.
(2) Provide a level of training adequate to enable effective use of LEDS and associated systems.
(3) Function as the NCIC Control Terminal Agency and the NLETS Control Terminal Agency for the State of Oregon.
(4) Assist and train criminal justice agencies in the development of information from LEDS and associated systems for use in criminal investigations.
(5) Develop and maintain linkages with the Driver and Motor Vehicle Services Branch (DMV), the State Marine Board, the Public Utility Commission, and other non-criminal justice agencies to make appropriate information available to Oregon criminal justice agencies to assist in the enforcement of state criminal and traffic laws and regulations.
(6) Provide staff support to the Law Enforcement Data System Advisory Committee.
(7) Develop and operate the State Uniform Crime Reporting Program to collect crime statistics information from local and state law enforcement agencies; provide information to the public, the Governor, the Legislature, contributing agencies, and others who have a responsibility for the prevention or reduction of crime.
(8) Provide monthly and annual Oregon crime statistics information to the Federal Bureau of Investigation to satisfy national uniform crime reporting program requirements.
(9) Operate a program of record validation, quality control, and audits to ensure that records entered into LEDS and NCIC files by user agencies are kept accurate and complete and that compliance with state and national standards is maintained.
(10) Provide assistance and information access to non-criminal justice user agencies for statutory licensing, employment and regulatory purposes and for other purposes authorized by law.
Stat. Auth.: ORS 181.730(3)
Stats. Implemented: ORS 181.730
Hist.: OSP 1-1995, f. & cert. ef. 8-15-95; OSP 2-1998, f. & cert. ef. 10-6-98

257-015-0050
User Responsibilities
(1) "User Agreement" Any agency using a terminal to access the Law Enforcement Data System, whether directly or through another agency, is responsible for adhering to all applicable LEDS rules and policies and must sign an agreement with LEDS to that effect.
(2) "Record Validation" Any agency that enters information into LEDS or NCIC files is responsible for the accuracy, timeliness and completeness of that information. LEDS will send a record validation review list, regularly, to each agency. Validation is accomplished by reviewing the original entry and current supporting documents. Recent reconsultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual also is required with respect to the Wanted Person, Missing Person, and Vehicle Files. In the event the agency 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 original entry in the file. Validation procedures must be formalized and copies of these procedures must be on file for review during a LEDS or NCIC audit. When the agency has completed the validation they must return a signed certification of their validity within an appropriate time as established by LEDS.
(3) "Minimum Training" Each agency employee who operates a terminal to access the LEDS network must complete a LEDS System Training Guide at a level consistent with the employee's duties. Pursuant to procedures outlined in the LEDS Operating Manual, the agency LEDS Representative must issue a Training Guide to such employees within ten (10) calendar days of the person beginning to access LEDS via a terminal. The Training Guide must be completed within 60 calendar days from the date of issue. Each employee who operates a terminal to access LEDS must be re-certified by the agency every two years per schedules and procedures as prescribed by LEDS.
(4) "Hit Confirmation" When another agency receives a positive record response (Hit) from LEDS or NCIC and requests confirmation of the status of the record (warrant, stolen vehicle, etc.), the agency responsible for entry of the record must respond within 10 minutes for *urgent* hit confirmation requests or within one (1) hour for *routine* hit confirmation requests, with an answer indicating the status of the record or indicating when the record status will be confirmed.
(5) "Agency LEDS Representatives" The agency administrator of each agency with terminal access to LEDS must designate an agency LEDS Representative who shall be the primary contact for all matters relating to use of LEDS by the agency. The agency LEDS Representative must complete the **LEDS System Training Guide** before a training guide will be issued to other agency employees. The agency LEDS Re presentative must complete a **LEDS System Training Guide** at the highest level required by any person in the agency before a training guide will be issued to other agency personnel. Every LEDS Representative must satisfactorily complete no less than the **Inquiry Level Training Guide**.
(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.
Stat. Auth.: ORS 181.730(3)
Stats. Implemented: ORS 181.730
Hist.: OSP 1-1995, f. & cert. ef. 8-15-95

257-015-0060
Information Access and Dissemination
Information is made available to LEDS users from various sources and agencies, including LEDS and other state information system files, motor vehicle departments, NCIC, Oregon State Police Identification Services Section, etc. Each user must observe any restrictions placed on the use or dissemination of information by its source. It is LEDS' responsibility to advise user agencies of any restrictions, which apply to any information, accessed via the Law Enforcement Data System.
(1) Investigative Files: Information from investigative files maintained by LEDS, NCIC, or other agencies is for criminal justice use only and is not to be disseminated to any person for other than an official criminal justice purpose. Inquiries from the public regarding the status of an investigative file should be referred to the agency holding the case.
(2) Oregon Computerized Criminal History Records (CCH):
(a) Oregon criminal history records are available via LEDS, from the Oregon State Police Computerized Criminal History Files, to agencies, which are authorized by the Oregon State Police.
(b) All agencies accessing the Oregon CCH files must have a signed agreement with the Oregon State Police and must adhere to Oregon Administrative Rules (OAR) 257-010-0025 through 257-010-0050 adopted by the Department of State Police.
(3) Federal Bureau of Investigation - Interstate Identification Index (FBI-III): The Federal Bureau of Investigation maintains the Interstate Criminal Identification Index, which is available through LEDS. Access to this information is restricted to criminal justice agencies, as defined in OAR 257-015-0015(5), in the discharge of their official responsibilities, or to non-criminal justice agencies which provide services to criminal justice agencies, and which have signed a management control agreement with a criminal justice agency.
(4) Oregon Motor Vehicle and Driver Records:
(a) Oregon motor vehicle registration and driving records are the responsibility of the Oregon Department of Transportation, Driver and Motor Vehicle Services Branch (DMV). Government agencies in Oregon have access to these records via LEDS for authorized criminal justice purposes and for licensing, employment and regulatory purposes specifically authorized by State Law and approved in writing by DMV. Communication, dissemination, or use of this information for other than authorized purposes is prohibited.
(b) Authorized purposes do not include inquiries for the collection of taxes and parking violation fees or fines;
(c) Authorized purposes are specifically defined as follows:
(A) Enforcement of state traffic and criminal laws, and regulations;
(B) Identification of vehicles, which have been towed or impounded by police;
(C) Screening of prospective or present agency employees who will have access to LEDS equipment or information;
(D) Identification of vehicles or individuals associated with criminal investigations;
(E) Review of driving and registration records for prosecution and sentencing functions;
(F) Processing of school bus driver applications by the State Department of Education;
(G) Access to vehicle registration information by fire and rescue agencies in emergency situations where waiting for the availability of a law enforcement officer would compound the emergency;
(H) The identification of vehicles or individuals associated with the Weighmaster enforcement function;
(I) Inquiries for licensing, employment and regulatory purposes authorized by State law and approved in writing by DMV.

(d) Inquiries for any purpose other than those specified in paragraphs (4)(c)(A)-(4)(c)(I) of this section must be directed to the department of Transportation, Driver and Motor Vehicle Services Branch (DMV) by telephone or by mail, together with the proper fee or account number. Violations of these policies may result in the suspension or termination of motor vehicle records access.
(5) National Law Enforcement Telecommunications System (NLETS) Access: NLETS provides a link to criminal justice information systems in other states for the purpose of point-to-point communications between criminal justice agencies and for access to information systems. Access to criminal history records in other states, via NLETS, is restricted to criminal justice agencies, as defined in OAR 257-015-0030(5). Access to motor vehicle records in other states and the use of the agency-to-agency communication facilities may be limited by NLETS policies or policies in other states.
(6) Corrections Offender Records:
(a) The Corrections Offender File contains records of persons under the active supervision (probation, parole, other non-custodial supervision) of a state or local or federal corrections agency. Entries and changes to this file are the responsibility of the supervising state or local or federal corrections agency.
(b) Access to Corrections offender records via LEDS is restricted to criminal justice agencies for criminal justice purposes.
(7) Administrative Messages: An administrative message (AM) is a free text message, from one agency to one or more agencies.
(a) All administrative messages transmitted via LEDS must be by the authority of an authorized user.
(b) Use of administrative messages via LEDS is restricted to criminal justice purposes, with the following exceptions:
(A) Emergency public safety messages such as storm warnings, disaster warnings, road conditions, etc., may be transmitted by agencies with responsibilities in these areas.
(B) Emergency inter-departmental and intra-departmental non-criminal justice business messages may be transmitted at any time. Non criminal justice non-emergency business messages may be transmitted between 12:00 and 1:00 p.m. Monday through Friday, between 5:00 p.m. and 8:00 a.m. Monday through Friday, or any time on weekends and holidays.
(C) Messages from agencies recruiting for personnel are not to be sent as all points bulletins or area broadcast messages. They may be sent to LEDS. LEDS will then compile and transmit a consolidated bulletin weekly, or as needed.
(D) Messages from agencies regarding equipment wanted, or for sale, are not to be sent as all points bulletins or area broadcast messages. They may be sent to LEDS. LEDS will then compile and transmit a consolidated bulletin weekly, or as needed.
(E) Announcements of meetings of recognized criminal justice professional organizations may be sent by the authorized officers of such organizations.
(F) Announcements of official inter-departmental or intra-departmental activities such as training classes, shooting tournaments and other organized professional competition or sports events, public service projects, etc., may be sent by the agency responsible for scheduling the activity. The addressees of such announcements should be limited to those participating in, or interested in, the activity.
(G) Use of LEDS for promotion of a particular political point of view (lobbying) regarding proposed legislation, elections, or other issues is prohibited. However, this does not preclude information announcements of association meetings, hearings, or other forums where such issues will be discussed.
(H) Non-criminal justice LEDS user agencies may send and receive administrative messages when the purpose of such messages is within the context of their statutory or designated authority and approved purpose for LEDS access.
(8) Demonstration or Display of Records: Any public demonstration involving the display of records or communication received via LEDS shall be confined to information pertaining to the individual performing the demonstration or to appropriate test records.

Stat. Auth.: ORS 181.730(3)
Stats. Implemented: ORS 181.730
Hist.: OSP 1-1995, f. & cert. ef. 8-15-95; OSP 2-1998, f. & cert. ef. 10-6-98

257-015-0070
System Security and Privacy
The data stored in the LEDS, NCIC, and other criminal justice information system files is documented criminal justice information. This information must be protected to ensure its integrity and its correct, legal and efficient storage, dissemination and use. It is incumbent upon and agency operating a LEDS terminal, or a terminal on another system which has access to the LEDS network, to implement the procedures necessary to make the terminal secure from any unauthorized use. All agency personnel authorized to access the LEDS network must be instructed in the proper use and dissemination of the information.
Stat. Auth.: ORS 181.730(3)
Stats. Implemented: ORS 181.730
Hist.: OSP 1-1995, f. & cert. ef. 8-15-95

257-015-0080
Criteria for Terminal Access to LEDS
LEDS uses the following criteria to determine if an agency qualifies for placement of a LEDS terminal, or for access via a terminal on another system, which has access to the LEDS network. Questions about whether or not an agency meets one of these criteria or whether LEDS access is appropriate will be resolved by the LEDS Advisory Committee:
(1) The agency is a criminal justice agency as defined in OAR 257-015-0030(5); or
(2) The agency is a service agency which provides computer services, dispatching support, or other direct support service to one or more criminal justice agencies, and which has signed a management control agreement with a criminal justice agency; or
(3) The agency is a non-criminal justice agency with a statutory requirement to use information or capabilities which may be available via LEDS, and use of a terminal by the agency will not adversely affect criminal justice agency users, and use of the terminal will be for a criminal justice purpose as defined in OAR 257-015-0030(6); or
(4) The agency is a non-criminal justice agency which provides information or capabilities needed by criminal justice agencies for a criminal justice purpose, and use of a terminal will improve the ability to provide such information or capabilities; or
(5) The agency is a non-criminal justice agency with statutory requirement to use information or capabilities which may be available via LEDS, and use of a terminal by the agency will not adversely affect criminal justice agency users, and use of the terminal will be for the specific non-criminal justice purpose(s) for which the agency is authorized access to the information or capabilities available via LEDS, and the agency has been approved for terminal access by the LEDS Advisory Committee.
Stat. Auth.: ORS 181.730(3)
Stats. Implemented: ORS 181.730
Hist.: OSP 1-1995, f. & cert. ef. 8-15-95; OSP 2-1998, f. & cert. ef. 10-6-98

257-015-0090
Criteria for Revocation of Terminal or Informational Access to LEDS
The authorization of any agency to access the LEDS network or associated systems or to retain access is subject to revocation or cancellation by LEDS on the following grounds:
(1) Violation by the agency or a by a member of the agency of any state statute, administrative rule, or policy pertaining to the use of LEDS or associated systems.
(2) Violation of the security of the LEDS system.
(3) Accessing, retrieving or using information from or through the LEDS system for non-official or unauthorized purposes.
Stat. Auth.: ORS 181.730(3)
Stats. Implemented: ORS 181.730
Hist.: OSP 1-1995, f. & cert. ef. 8-15-95

257-015-0100

Criteria for Computer Access to the LEDS Network

(1) A local or state government computer center may be given direct access to the LEDS network if the agency operating the computer is a criminal justice agency. If the agency operating the computer is not a criminal justice agency, then there must be a current management control agreement in effect between the computer center management and one of the criminal justice agencies served by the computer center.

(2) The criteria for allowing terminal access to LEDS are described in OAR 257-015-0080. A local or state computer system connected to LEDS may allow such access after giving written notification to the LEDS Director, including the identification of the agency requesting access, the terminal identifier, and other information needed by LEDS to ensure proper authorization.

Stat. Auth.: ORS 181.730(3)

Stats. Implemented: ORS 181.730

Hist.: OSP 1-1995, f. & cert. ef. 8-15-95; OSP 2-1998, f. & cert. ef. 10-6-98

Alphabetical Index by Agency Name
Numerical Index by OAR Chapter Number
Search the Text of the OARs
Questions about Administrative Rules?
Link to the Oregon Revised Statutes (ORS)
Return to Oregon State Archives Home Page