

2013  
Fall

OREGON  
CRIMINAL JUSTICE  
INFORMATION SYSTEMS  
NEWSLETTER

# CJIS



**Patricia Whitfield**  
CJIS Division Director  
503 934-2305

**Captain Tom Worthy**  
CJIS Systems Officer  
503 934-0266

**Jeff Bock**  
OUCR Manager  
503 934-2342

**Greg Verharst**  
CJIS Info. Sec. Officer  
503 378-3055 x 55002

**Dan Malin**  
LEDS Auditor  
503 934-0301

**Jennifer Hlad**  
Training Coordinator  
503 934-2341

**Cindy Comstock**  
Help Desk Manager  
503-378-3055 x 55001

**24/7 Help Desk**  
503 378-5565

**24/7 Help Desk Fax**  
503 588-1378

**CJIS Division Fax**  
503 378-2121

**CJIS Division's new  
Mailing Address:**  
3772 Portland Rd. NE  
Building C  
Salem, OR 97301

The OSP CJIS Division	P.1
A Letter From Cpt. Worthy	P.2-4
UCR Update	P.4-5
LEDS Auditing & Agency File	P.6-7
Training & Recertification	P.8
Nlets Investigative Tool	P.9
N-DEx & CJIS Training	P.10-11
CJIS Auditing Information	P.12-13
IT Service Contacts	P.14-15

## The OSP CJIS Division

We would like to introduce you to the new face of LEDS, we are now the Criminal Justice Information Systems (CJIS) Division. This is just one of the big changes we have undergone as an agency in the past year. We have also physically moved locations combining forces with the team at OSP ID Services. Please take a minute to review our new points of contact listed for you on the side margin.

We have several new faces representing our agency, Patricia Whitfield & Captain Tom Worthy have taken on the leadership of the CJIS Division. Patricia Whitfield, longtime Director of ID Services, has taken over the administrative leadership of the CJIS Division and Captain Worthy has filled the role of CJIS Systems Officer for the State of Oregon. Patricia and Captain Worthy both bring with them long and distinguished careers with the State Police.

We would like to welcome Greg Verharst our new CJIS (ISO) Information Security Officer. Greg has already begun traveling around the State of Oregon conducting onsite audits to ensure your agency is in compliance with the Federal CJIS Security Policy version 5.2. Jennifer Hlad (formally Jennifer Ferris) has accepted a position leading the Training Unit. Jennifer has been busy conducting regional training events in Bend, Troutdale, Newport and Salem. Next on the agenda is a training in Eugene on 01/07/2014. Contact Jennifer if you would like to discuss hosting a training event at your agency.

Please help us welcome all of our new staff as they establish themselves in their new roles within the OSP CJIS Division.

## A Message From Captain Tom Worthy — CJIS Systems Officer

Greetings,

I sit on the Criminal Justice Information Services (CJIS) Western Working Group (WG) as your CJIS Systems Officer or State CSO. This WG meets twice per year to discuss and vote on, in detail, topic papers that are presented to the FBI for consideration of policy change to all things CJIS. Policy changes are reviewed by the working groups and go through several groups and the Advisory Policy Board (APB) before final approval and implementation by the Director of the FBI. The Western WG consists of two representatives from each of these states and territory: HI, Guam, AK, WA, OR, CA, AZ, NM, TX, CO, UT, NV, WY, MT, and ID. There are four regional working groups and one federal working group.

Part of my duty as CSO is to solicit topic papers. Here's where you come in. If you or your agency feel like a change needs to be made by the FBI for any CJIS program, this is your opportunity to give input.

IF YOU HAVE AN IDEA, please fill out the attached Topic Paper Solicitation Form and send it to me or Brian Wallace of the Marion County Sheriff's Office. Brian is your local representative and my counterpart on the Western Working Group. You can type your own documents as well if you wish. I will ensure it is passed along to the appropriate FBI staff for evaluation and consideration. Both Brian and I sit on the WG and would really like our law enforcement partners in our great State to participate and shape CJIS. Brian and I work very well together and are there to advocate for you.

IF YOU AREN'T SURE of whether or not your idea is "good" or if it falls under the auspice of CJIS, don't hesitate to give me a call and we can talk it over. If I don't know, I will find out. These systems are complex.

What types of topics are presented?

Many! It runs the whole gamut. Some of the 24 topics we reviewed a couple weeks ago included:

1. Whether a DNA indicator field should be included w/in a criminal history record, and who is responsible for modifying the field
2. Posting of federal disposition information to the IAFIS and eliminating related arrests without court data
3. Defining Domestic Violence for the UCR program
4. Exceptional clearance criteria (for credit card fraud)
5. Expanding the use of the NICS for Criminal Justice hires

(Continued on page # 3)

## Captain Worthy Continued...

6. Encryption standards for CJ info

7. Request from the Department of Homeland Security of Biometric Identity Management re: IDENT searches by partner countries (expanding info sharing with Canada, New Zealand and Australia, in addition to the UK Visa program)

You can see topics range from National Security issues to Uniform Crime Reporting, NCIC fields, CJIS security, etc. Each topic is discussed, sometimes at great length. It is very interesting to see the different perspectives, especially from system officers who are more on the technical side of CJIS issues, and local law enforcement representatives who are more "operational" minded.

What are the FBI programs CJIS oversees where a working group could vote on a potential topic or policy change that directly affects the LE community? NCIC (National Crime Information Center) - All functions of NCIC, including KST (Known or Suspected Terrorist file entries), stolen vehicles, guns, missing persons, protection orders and many, many more.

UCR (Uniform Crime Reporting) - mandatory reporting of certain arrests, crimes, crime analysis data and other information. Local agency data is submitted to LEADS on a monthly cycle and each year LEADS submits all Oregon information to the FBI for the annual "Crime in the U.S." publication.

IAFIS (Integrated Automatic Fingerprint Identification System)

NICS (National Instant Check System) - for handgun purchases

LEO (Law Enforcement Online) - an online forum and information center for all LE where you can sign up for certain access to information, etc.

NDex (National Data Exchange) - a free FBI database that connects all state local agency records who's state "LEADS" system reports certain expanded information through the UCR process. More information is shared by reporting in NIBRS format (National Incident Based Reporting System). Look at this as a national database similar to that of "Coplink" where you could run a name through another jurisdiction or state and find out if local records exist.

I am very honored to be a part of this WG and to actively participate in discussion of various topics. Rest assured that all of my votes and input are based on what is best for Oregon, the U.S. and our law enforcement partners, officer safety...and common sense. I see my participation as an opportunity to make positive changes for the LE community as a whole and ultimately make our communities safer.

## Captain Worthy Continued...

There are time lines for submitting a topic. Topic papers to be presented in Spring of 2014 are due before Sept. 23. If you miss the deadline the topic will hold until August 2014. You don't need to worry about any of this unless you have a hot topic or issue.

If you have questions please contact me directly (contact details below for Brian and I). Additionally, feel free to pass this info along to anyone in your agency who may have a need for a topic (warrants, records, patrol, IT). Myself and Brian very much encourage your participation, and I am willing to help you in any way I can.

Thanks for reading...  
Sincerely,

Tom

Captain Tom M. Worthy  
Oregon State Police  
General Headquarters  
255 Capitol St. NE 4th Fl.  
Salem OR 97310  
PH- 503-934-0266  
Tom.Worthy@state.or.us

Brian N. Wallace, Chief Civil Deputy  
Operations Division  
Marion County Sheriff's Office  
Courthouse - 100 High Street NE  
PO Box 14500, Salem, OR 97309  
PH- 503-589-3271  
BWallace@co.marion.or.us

## Oregon Uniform Crime Reporting

**The clock is ticking. In only 36 months the old OUCR-1 format is set to retire.** If you are making agency report management changes, please contact Oregon UCR for guidance.

Identity Theft has become a big headache for law enforcement in recent years. Usually the victim lives in one jurisdiction and the offender lives somewhere else. In many cases, deciding which agency is supposed to report the Offense has been confusing. The solution is fairly straight-forward. The jurisdiction where the offender used someone else's identity is the reporting agency.



For example, let's say that a Victim who lives in Canby reports that someone has been using his identity to make on-line purchases. The Offender lives in Gresham. He made the on-line purchases from his Gresham residence.

(Continued on page # 5)

## UCR Continued...

Gresham PD is the agency responsible for reporting the ID Theft to the OUCR Program because the Offense(s) occurred within their jurisdiction.

Okay, suppose the Offender (who still lives in Gresham) went in person to Bend and made purchases, or in some other way benefitted by using the Victim's identity. Now it's up to Bend PD to report the Offense(s) because the Offender's location when committing his crime(s) is within their jurisdiction.

As always, there's an exception. Suppose our Victim lives in Canby, but the offender is in Pakistan. Obviously, there is no way that Pakistani police are going to investigate the incident, nor will any police officer from Oregon travel to Pakistan. In a situation like this, it falls back to the agency where the Victim resides to take the Victim's complaint and report it to OUCR in order to collect the Offense.

Just remember that it is (usually) the location of the OFFENDER when he/she committed the crime(s) that determines who reports the Offense(s). The exception being when it is impossible for the victim to report the Offense to the law enforcement agency where the Offender is located (either because the location is unknown or is outside of the country).

That's a perfect segue to the next item: who reports in multi-jurisdictional incidents? As complicated as these incidents can become, it's simply the responsibility of the law enforcement **agency that has jurisdiction over the location where the Offense(s) occurred** to make the report to the OUCR Program. That's an FBI UCR rule.

Suppose Medford PD, Phoenix PD and Talent PD form a drug task force. Two under-cover officers, one from Medford and one from Talent, make a buy of some heroin from a house in Phoenix and arrest 5 subjects on various drug charges. Since the location of the incident was in Phoenix, it falls to Phoenix PD to report the incident to the OUCR Program.

OUCR has a new email address. If you have a question or concern and you're not sure it should go to Jeff, Nancy or Susan, send it to [osp.oucr@state.or.us](mailto:osp.oucr@state.or.us) and one of us is sure to see it and make certain the correct person addresses your concern.

# AUDITS

Auditor Dan Malin made good progress in 2013 with audits completed in Lincoln, Yamhill, Lane, Washington, Wallowa, Baker, Malheur, Harney, Jefferson, Klamath, Lake and some of Multnomah County. Hood River and Wasco Counties will be audited in December. Polk County will be up first in 2014 in January, and Dan will continue to conduct more Multnomah County audits when there is time. Dan has Clackamas County scheduled for February and Douglas County in March. As always, look for Dan's audit letters 30 days in advance of the audits. For information on the audit process please visit our secure website and refer to the LEDES Representative Manual Section, then select the link for LEDES/NCIC Audit Procedures and Reports.

Some of the frequent issues Dan has encountered during audits are:

- No Agency Record Validation Policy
- Running Criminal Histories for External Agencies with no Legal Basis
- Running Criminal Histories with the Wrong Purpose Code
- Incorrect Extradition Limitation Information on Warrants
- Missing Person Juvenile (EMJ) Records not entered within 2 Hours
- Dental Record and DNA Information Missing in Missing Person Records
- LEDES Training Records not up to date
- Fingerprint or CJIS Security Flag Issue

If you suspect your agency might be having issues in any of the above listed areas, please contact Dan so he can complete a review and work with your agency to resolve the issue before too much time has passed. Additionally, Dan has boilerplate validation policies for any agency that might need to incorporate this vital process into their organization.

Reminder - The LEDES Auditor handles all internal investigation/system misuse investigation requests personally.

Don't hesitate to contact Dan Malin at 503 934-0301 or email [Dan.Malin@state.or.us](mailto:Dan.Malin@state.or.us) with any questions or requests for assistance.

# AUDITS

## Audit Issue - Extraditable Warrant Extradition Limitations

We are seeing a number of extraditable warrants where the Extradition Limitations field (EXL) in LEDS does not match what is in NCIC. So in LEDS it might show code 2 Limited Extradition, in NCIC it shows code 1 Full Extradition. Additionally, it might show Limited Extradition, in either or both, but in the MIS field it reads NATIONWIDE SERVICE, or the extradition limitations, e.g. the states from which extradition is authorized are not entered.

All warrants are validated 60 – 90 days after initial entry and again, annually during the anniversary of the month of entry. To validate a record in LEDS/NCIC the entering agency must run the record. You must first confirm that the record is still in LEDS and NCIC. When you run the record these errors are easy to identify and are relatively easy to correct – generally a modification of the EXL and MIS fields is all that is required.

If your agency has not been running records of extraditable warrants during annual validation, please modify your agency validations policy to include this step, and visit with your records validation staff to ensure they are looking at the records. This will ensure that a hit confirmation on your warrant will be handled quickly and easily.

### Keeping your LEDS agency file up-to-date:

Has your agency moved? Have your email addresses changed? Have you appointed a new LEDS Representative, Agency Administrator and/or agency technical point of contact? If any of these apply to your agency please make sure your LEDS agency ORI file reflects your correct information. The OSP CJIS Division uses this information to send out email directives, invitations to training events, your agency validation files and much more. To submit an update to your agency file please complete the online customer service form by visiting our website:

<http://www.oregon.gov/OSP/CJIS/pages/index.aspx>



**Select: LEDS Customer Service Forms**

**Login Credentials:**

**Username: OSPCJIS**

**Password: IwoJima**

*Please note both username & PW are case sensitive*

## Consider LEDS Recertification Needs

As the New year approaches be mindful of the need to ensure your employees LEDS Certifications are up to date. When we rolled out the online recertification tool Training had advised LEDS Representatives to rely on the automated email notifications. This is no longer the case. Because these email notifications have become increasingly susceptible to email spam filters, the automatic notifications are considered a courtesy and should not be relied upon as your sole reminder to recertify your LEDS users. Please proactively track your LEDS training expirations and administer needed training. You can easily view your employees LEDS certification expiration date by querying LEDS Training records by Employing Agency. This function is available by both the "QTR" transaction and via free format:



**QTR.OR0370000.EMP/OR0370000.SRT/A**

YOUR ORI HERE

THE AGENCY YOU WANT TO LIST HERE

This LEDS command will list all of the employees active for the directed ORI in LEDS.

A few additional reminders from the Training Unit:

- NexTest and LEDS **DO NOT** talk to each other. The LEDS Training records need to be updated manually to reflect the recertification testing dates. This is completed by ETH (Enter Training History) transaction covered in 3.11.3 of the LEDS Rep. Manual.
- The NexTest username and password are case sensitive and automatically set as your agencies ORI which contains both zero's and the capital letter "O".
- When creating new user accounts in the NexTest system, LEDS Representatives cannot add expiration dates to the NexTest records for new employees. The Training Unit does this once we receive the copy of the test answer sheet, we will update their record showing the expiration date. If you don't send in their test answer sheet, their record cannot be updated!
- **DPSST is now only tracking F6 credit for sworn personnel - you must submit your own F6 forms directly to DPSST for credit for LEDS Training activity.**

Please contact Jennifer Hlad in the CJIS Training Unit with any questions: 503-934-2341

# License Plate Reader Databases

9

## Available via Nlets Connection to NVS

NVS working with Locator Technologies, has partnered with an LPR company to provide Law Enforcement Agencies (LEA) access to a Central Repository of LPR data from private mobile and stationary LPR machines. The companies collecting these reads include towing and repossession companies, parking lots, garages, and toll way systems. LEAs may utilize this information at no cost to augment and/or initiate criminal investigations. **Presently Oregon is not contributing information to this database**, but Law Enforcement Agencies will have access to other contributing states.

The National Vehicle Service (NVS) also supports the Nlets 'RQ' message key to query their LPR database. Nlets users, in addition to being able to query the CBP Crossing LPR database via destination 'NA,' can now also send 'RQ's to destination 'VS' to query NVS' database containing nearly 300 million LPR reads with 30 million being added per month.

In addition to allowing LEAs access to the database, NVS proactively searches the database against the stolen vehicle file provided by the FBI. Knowing the location of a stolen vehicle prior to or shortly after its theft will greatly enhance LEA's capabilities.

### Question: How do I run this transaction?

Answer: To utilize this new Nlets functionality, using the RQ mask or screen (out of state registration query by license plate) enter 'VS' in the State Field of the 'RQ' function, as well as the plate number and license year (standard Nlets 'RQ' query). A positive response to your query will be similar to the below provided sample.

**If there is no match for your plate, then your response will indicate that there is no match for your plate.**

Contact the Nlets network for more information at: 800-528-4020

```
RR.VANVS005V
08:59 03/29/2010 44914
08:59 03/29/2010 00604 VANVS006V
*JSPI00MX00
TXT
Vehicle license plate number 619WCX was captured by mobile license
plate recognition on March 21, 2010 near the intersection of W Forest
Brook Dr AND Woodside Rd, Casselberry FL.

To access the complete LPR data record including other additional
historical LPR scans, vehicle images and satellite map overlays,
please proceed to the following Internet Website: http://nvls-lpr.com/nvls or http://www.platenet.net

** CAVEAT **
This is lead information ONLY to assist with your investigation and
should NOT be used for non-law enforcement purposes. Should you
require additional assistance with this RESPONSE, please contact
National Vehicle Service at 866-687-1102.
```



Information sharing has become one of the most critical elements of coordinated criminal justice enforcement efforts, but the ability to share information electronically between even adjacent agencies is in many cases both technologically and fiscally unfeasible. With the implementation of the new Oregon State Police Records Management System (RMS), OSP will take a major leap forward in information sharing through direct participation in the FBI National Data Exchange Program (N-DEX).

N-DEX is the FBI system that provides law enforcement agencies with a powerful new investigative tool to search, link, analyze, and share criminal justice information such as, incident/case report and arrest data, booking and incarceration data, probation/parole data, and expanded DOJ data sources on a national basis to a degree never before possible. N-DEX allows participating law enforcement agencies to detect relationships between people, places, things, and crime characteristics, and link information across jurisdictions. N-DEX has been developed in collaboration with the law enforcement community, and is currently accessible to authorized users within law enforcement and criminal justice communities.



Oregon law enforcement agencies have almost 900 thousand records in N-DEX available for sharing on a national level. There are over 90 million records in N-DEX itself which are directly available for law enforcement purposes.

N-DEX additionally provides contact information and collaboration tools for law enforcement agencies that are working on cases of mutual interest. Ownership of data shared through N-DEX remains the property of the law enforcement agency that submits it. N-DEX supplies controls to allow law enforcement agencies to decide what data to share, who can access it, and under what circumstances allowing agencies to participate in accordance with applicable laws and policies governing dissemination and privacy.

Oregon State Police information will flow directly from their new RMS, to a computer system at LEDS, and then on to the FBI for inclusion in N-DEX. All law enforcement agencies in the nation will then have instant access to OSP information and OSP personnel will be able to make information correlations with our data and the data that resides in N-DEX. Searching for that information in N-DEX uses a simplified user interface similar to an internet search engine like Google.

# NDEx Continued...

11

The success of these correlations have already been proven in Oregon when a Hood River agency used N-DEx and found a homicide suspect they were searching for living in California. They successfully arrested, extradited, and convicted the person of the homicide.

The process to access N-DEx begins initially with obtaining an FBI Law Enforcement Online (LEO) account through LEO.gov (<http://www.leo.gov/>).

Once you have a LEO account follow the procedures found on the LEDS website for N-DEx access ([http://egov.oregon.gov/OSP/CJIS/docs/NDEX\\_APPL\\_PROCEDURE.pdf](http://egov.oregon.gov/OSP/CJIS/docs/NDEX_APPL_PROCEDURE.pdf)).

While access to N-DEx is currently via LEO, they have developed a secure portal that will support access from other systems. LEDS will work with N-DEx to determine if the portal capability is compatible with other state systems that are in development. LEDS is also implementing a process that will allow all Oregon law enforcement agencies to submit an expanded set of data elements to N-DEx, emulating the capability that OSP will have with its new RMS, further expanding the capacity for Oregon law enforcement agencies to share information.

N-DEx is functioning now, has proven results, and best of all its free to use. For further information about N-DEx visit Leo.gov, the secure website, or contact Jeff Bock at 503-934-2342

## CJIS Security Awareness Training Directive

CJIS Security Awareness Training is required for all individuals with unescorted access, physical OR logical, to CJIS as stated in the FBI CJIS Security Policy. This directive is based upon the CJIS Security Awareness policy version 5.2 issued by the FBI. The policy states basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to Criminal Justice Information (CJIS).

The three types of CJIS training are defined as follows:

Level 1: Personnel with unescorted access to areas in which CJIS is processed.

Level 2: Personnel with terminal access to CJIS as part of their normal duties. (This training will be included in your LEDS Certification / Recertification process as of early 2014.)

Level 3: Personnel with access (physical or logical) to IT systems processing or storing CJIS. Access to the states online system is available at [CJIS Online](#). Instructions on how to log in and set up user accounts is available [here](#).

CJIS security training questions? Contact Jennifer Hlad at 503-934-2341

CJIS policy questions? Contact Greg Verharst at 503-378-5565 Ext. 5502

# CJIS Security Policy Audit Update:

Greg Verharst, the state CJIS ISO, has been auditing agencies for CJIS Security Policy compliance since August 2013. These audits are a required part of the FBI CJIS Security Policy, Section 5.11.2, that states auditors will "at a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies." About 580 terminal agencies currently operate in the state of Oregon.

These policy audits are designed to be an external, independent appraisal of the agency's technology systems, processes, and policies when accessing LEDS/NCIC systems. OSP is primarily concerned with assisting the agencies and is available to answer questions before, during, and after the security audits.

To date, Greg has completed about 50 audits. In general, Greg is finding that agencies are doing what they are supposed to be doing and how they are supposed to be doing it. Most of the findings reflect missing policies, processes, or procedures. Greg has compiled a list of sample policies that your agencies should have in place. These samples are found at <http://www.oregon.gov/osp/ID/Pages/cjis.aspx>.

However, during multiple audits one repeated area of concern is evident: the use of shared or generic accounts. This sharing of accounts is a severe policy violation and requires immediate attention. Whenever an agency provides shared/generic account access to LEDS, NCIC, or CAD/RMS systems that store/process CJI, there is a lack of accountability to the individual accessing that data. Your agencies must be protected from system misuse, loss, and inappropriate release of CJI. Your agencies must be able to identify every unique individual accessing CJIS data. The FBI CJIS Security Policy states the following requirements:

## **5.6.1 Identification Policy and Procedures**

Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified.

### **5.6.3.1 Identifier Management**

1. Uniquely identify each user

Please contact Greg Verharst, State CJIS ISO with any questions or concerns at: 503-378-3055 Ext. 55002



## CJIS Concerns - Windows Update

### **Window XP EOL/EOS Reminder:**

Remember that April 8, 2014, is approaching quickly. This April date marks the day that Windows XP Service Pack 3 (SP3) customers will no longer receive new security updates, non-security hotfixes, free/paid-assisted support options, or online technical content updates. In other words, any new vulnerabilities discovered in Windows XP after its "end of life" on April 8, 2014, will not be addressed by new security updates from Microsoft.

What does this mean to you, and how can it affect your agency? After speaking with the FBI and the ITSA Team, after April 8, 2014, any machine—physical or virtual—running the Windows XP operating system with access to FBI CJIS data will result in a noncompliance finding during an audit. Greg will also begin auditing to these standards as of April 9, 2014, while conducting state audits.

If you have PCs, laptops, MDTs, or any other device currently running the Windows XP operating system with access to FBI NCIC data, you should plan to upgrade these operating systems by April 8, 2014.

### **CJIS Security Policy List Smart Mailing List:**

Want to receive more CJIS Security news and information directly from the CJIS Division, please consider signing up for our list serve.

### **Signing up for the CJIS Security Policy Forum Mailing list:**

Signing up for the service is as easy as visiting <http://listsmart.osl.state.or.us/mailman/listinfo/cjissecuritypolicy> and entering your email address and clicking the Subscribe button. All other fields are optional.

Once you have signed up you will begin receiving email updates from our CJIS Security list serve group.



## Get To Know Your IT Customer Service Contacts

One of the biggest frustrations for agencies can be getting in contact with someone when technology goes wrong. Early in the Information Technology age, it was common for an entire offices' IT needs to be provided by one person or vendor. They supplied the computers, network services, software, customer service and communications - all in one package. If one had a problem with their computer, they called "Bob".

Today's information systems are much more diverse and complex. There is an array of vendors supplying specialized services to resolve specific system requirements that may only be a small piece of your overall IT infrastructure. The first step in any Disaster Recovery Plan is to know what you have and who to call.

Many agencies consider LEDS to be their IT provider. We configure network settings to allow your computers to talk to our servers, we set up your system identification codes, we train you in how to use the system and we have a 24/7 helpdesk to assist you with a wide variety of questions and problems.

However, it might surprise you to know that of the 28,200 device IDs we maintain at LEDS, only 479 of those are our direct "customers". The vast majority of people who use LEDS actually get their access LEDS from a private vendor.

LEDS is a statewide database – a repository for criminal history and criminal justice information. Access to that database comes from private companies that sell their programs, services and support to the CJIS community. The LEDS Helpdesk often gets calls from people reporting "Our LEDS is down." When we look at our systems, we find that LEDS is not down at all; but rather your vendor's connection to LEDS is down. In 2012, LEDS was down a total of 11 minutes for the year. This year, LEDS has only been down a total of 6 minutes to date (Oct 2013).

Regardless of the cause, when LEDS gets a call for help, we investigate and work with your vendors until the issue is resolved. This is no easy task. While we try to maintain current contact lists for all of our regional systems and vendors, the fact is people take other jobs, retire or move on. Often, we don't find these things out until one of your systems goes down" at 3 AM and we are trying to contact one of your system support personnel.

(Continued on page # 15)



**Patricia Whitfield**  
 CJIS Division Director  
 503 934-2305

**Captain Tom Worthy**  
 CJIS Systems Officer  
 503 934-0266

**Jeff Bock**  
 OUCR Manager  
 503 934-2342

**Greg Verharst**  
 CJIS Info. Sec. Officer  
 503 378-3055 x 55002

**Dan Malin**  
 LEDS Auditor  
 503 934-0301

**Jennifer Hlad**  
 Training Coordinator  
 503 934-2341

**Cindy Comstock**  
 Help Desk Manager  
 503-378-3055 x 55001

**24/7 Help Desk**  
 503 378-5565

**24/7 Help Desk Fax**  
 503 588-1378

**CJIS Division Fax**  
 503 378-2121

**CJIS Division's new  
 Mailing Address:**  
 3772 Portland Rd. NE  
 Building C  
 Salem, OR 97301

## IT Service Contacts Continued...

We encourage you to get to know your customer service contacts. The easy thing might be to just call LEDS and ask us to fix it. While we will certainly try, often we simply can't; as it is not our system. We can't access your accounts, usernames, passwords, system locks, computer logins or system access. Only your vendor and system administrators can do that. Get to know who those people are and use them as your first point of contact when you are having a system issue. If they can't resolve the problem, they will call us and we will work with them to resolve the problem.

Your system administrator is also your point of contact when you want to add/remove a LEDS user's access. Often, we received these requests from agencies which we do not provide LEDS access to. Again, while we are happy to call and assist you in determining who you should contact, valuable time is lost for everyone. Knowing who to contact in the event of an emergency, or for daily adding/removing of a LEDS user, saves everyone time and increases work productivity.

LEDS is here to help. We built our entire infrastructure around delivering CJIS data to your desktop. We encourage you to take some time today and familiarize yourself with your desktop administrators and their contact information, so you can call on them when you have an immediate problem. We work with scores of talented, knowledgeable and dedicated people at the regional systems to provide you with reliable and accurate information. Get to know your IT people and understand the role they play in your agency.

