



Specific questions or concerns should be directed to the appropriate Division:

Information and Communication Technology Division

Call Center
1-800-877-2897
Email:
isdhelp@mshp.dps.mo.gov

Criminal Justice Information Services Division

UCR Unit
(573) 526-6278
Email:
ucr@mshp.dps.mo.gov

Access Integrity Unit
(573) 526-6141

CJIS Training Unit
(573) 526-6141

CJIS Audit Unit
(573) 526-6278

CJIS Information Security Unit
(573) 522-3820

AFIS, Quality Control,
Sex Offender, CHS
(573) 526-6153

If you have a change in contact information, please contact the UCR Unit at the phone number listed above or CJISNews@mshp.dps.mo.gov

THE CJIS NEWSLETTER

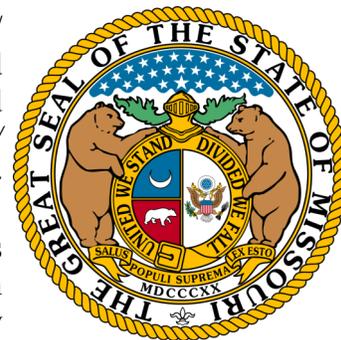


Criminal Justice Information Services

16-01

Newsletter Instructions; Policy Updates and Revisions

This newsletter should be divided into several sections. One section contains the pertinent information for MULES/NCIC Operators and should be removed and placed with the *MULES/NCIC Operational Manual* for future reference. Another section contains information for Uniform Crime Reporting agency



points of contact and should be removed and placed with the *Missouri Supplement to the UCR Handbook* and the *UCR Handbook*. Please ensure that all affected personnel receive an opportunity to review *The CJIS Newsletter* before it is sectioned out and placed with the designated manuals.

Mailbox Available for CJIS Newsletter Articles or Inquiries

Any Missouri criminal justice agencies that wish to submit content to the CJIS Newsletter (no editorials or commercial materials please) for distribution to the Missouri CJIS community, please feel free to do so by emailing articles to CJISNews@mshp.dps.mo.gov. Content will be subject to approval.

Additionally, please feel free to submit any questions or comments regarding the content of the CJIS Newsletter to CJISNews@mshp.dps.mo.gov. or 573-526-6278.

CJIS Newsletter Available Online

The CJIS Newsletters are always posted online on the same date they are released. The newsletters are available on the UCR website on the 'Downloads' page at:

<http://ucr.mshp.dps.mo.gov/ucr/ucrhome.nsf/downloads?openview&Count=50>

Alternatively, the newsletters are also published on the CJIS Launchpad under the CJIS Documents link for MULES users.

Missouri Highway Patrol Featured in Upcoming FBI Training Video

In April of 2016, the MSHP CJIS Division received notification from the FBI CJIS Training Unit that Missouri had been selected as the setting for a new training film on the NCIC Sex Offender File. This video will be released to law enforcement and criminal justice agencies nationwide to help NCIC users understand how Sex Offender information is stored and queried in NCIC.

The Missouri Capitol building, MSHP EVOC Track, Jefferson City's Riverside Park, the Cole County Sheriff's Office, MSHP Academy Gymnasium, and a private residence in Jefferson City were used as backdrops for several mock scenarios involving law enforcement coming into contact with registered sex offenders. Members of the CJIS Division got to play "bad guys" and officers from the Missouri Highway Patrol, Jefferson City Police Department, and Cole County Sheriff's department played the roles of Law Enforcement. In order to maintain anonymity, players will be uncredited and the scenes were shot in such a way as to not clearly reveal the faces of civilian actors. (Except for one sex offender role, which we hope won't be seen by any of J.D. Reece's friends or family without a proper explanation) The video will show officers coming into contact with sex offenders and then explaining briefly to the audience why a particular action was or wasn't taken.

MSHP CJIS personnel assisting the production of this film were: Lieutenant Steve Frisbie, J.D. Reece, Theresa Huhn, Kerry Creach, Chris Parr, Bruce Snider, Tiffany Garnett, John Rollins, Tammy Byrd, Pam Aberle, & Michelle Pfeiffer. Roles were also played by Communications Specialists Jan Edgell and Teneila Jackson of the Cole County Sheriff's Department.

Officers featured in the film are Corporal Kyle Green, Trooper Marylyn Dickens, and Trooper Bryan Salmons, all from Troop F, Officer David Mays, Sergeant Jason Payne, and Detective Curt Finke from the Jefferson City Police Department, and Corporal Todd Marsey from the Cole County Sheriff's Department.



Trooper Marylyn Dickens talks to the film crew prior to shooting a traffic stop scene for the FBI's new Sex Offender File training video.

CJIS CONFERENCE 2016

POLICY, PRACTICE, & INFORMATION SECURITY

October 4th, 5th, & 6th



3 days packed with information for all users of Missouri criminal justice computer systems on topics ranging from MULES/NCIC policy, Uniform Crime Reporting, and criminal justice information security, featuring speakers from:

- ◆ The Missouri State Highway Patrol
- ◆ The Federal Bureau of Investigation
- ◆ International Criminal Police Organization (INTERPOL)
- ◆ The International Justice and Public Safety Network (NLETS)
- ◆ National Missing and Unidentified Persons System (NamUs)
- ◆ National Insurance Crime Bureau (NICB)

Registration: \$225

Single Day Passes: \$90

Registration fee includes all training and organized social events including breakfast on the second and third day of the conference and lunch on the first and second day. Recertification and TAC Meeting credit will be available.

Late registration: After Sept. 5th full conference registration increases to \$275. Day passes increase to \$125.

Lodging rate is \$89 per night if booked prior to September 5th. Reservations must be made directly with Tan-Tar-A. Call (800) 826-8272 or follow the link on the registration website. A link can also be found on the CJIS Launch Pad.

Call Chris Parr at (573) 526-6153 ext. 2774 with any questions.

TO REGISTER

www.regonline.com/mocjisconference



Security Awareness Training

MSHP Information Security Unit

Phone: 573-522-3820

cjissecurity@mshp.dps.mo.gov

Security awareness training is required for all persons with unescorted access to criminal justice information (CJI). This training must be completed within six months of the hire date and every two years thereafter. There are several types of training that must be administered depending on the employee's role:

PERSONS WITH NO LOG ON TO THE SYSTEM

- Examples: Custodial Staff, Shredding Companies, Contractors, Maintenance Personnel
- Required Training: Level 1
- Training is received through CJIS Online

PERSONS WITH A LOG ON TO THE SYSTEM

- Example: MULES Users
- Required Training: Level 2
- MULES users receive security awareness during MULES certification courses and TAC meetings

PERSONS WITH INFORMATION TECHNOLOGY ROLES

- Examples: IT Personnel, CAD Vendors, RMS Vendors, Contracted IT Personnel
- Required Training: Level 3
- Training is received through CJIS Online

CJIS ONLINE- www.cjisonline.com

CJIS Online is a web based training that is accessible outside of the MULES network. The agency TAC or LASO must contact the MSHP Information Security Unit (ISU) to enroll the agency in the training. The agency will be added to the system by the MSHP ISU and the TAC or LASO will be assigned as the agency administrator. The instructions for operating the system are located on the CJIS Launchpad.

The agency administrator can enter anyone at the agency or any vendor into the system to take the training. The agency will assign Level 1 or Level 3 training. Emails will be sent when the user must complete the training again.

Vendors

Agency admins can view and add vendors in CJIS Online. If a vendor has previously taken the training at another agency, the agency admin can access all vendor records to verify the training of each vendor employee.



2015 FBI CJIS SECURITY POLICY CHANGES

MSHP INFORMATION SECURITY UNIT

Phone: 573-522-3820

cjissecurity@mshp.dps.mo.gov

The FBI CJIS Security Policy version 5.4 was released on October 16, 2015. Several new requirements and language changes for virtual escorting, user-based certificates, encryption, and virtual environments are included in the updated version. All changes and additional requirements are reflected in MSHP Technical Security Audits. Below is a brief description for these changes.

Requirements Priority Tiers:

The tiers provide a baseline for those requirements that must be met immediately and those that may be delayed pending CSO approval.

Tier 1 requirements must be met by a system before a CSO can allow connections to the state system.

Tier 2 requirements must be met by the date indicated in the plan approved by the CSO.

Language:

Police vehicle changed to Criminal Justice Conveyance

Law-enforcement officer changed to Criminal Justice Professional

Policy Area 5.5.6

Remote Access: New requirement to identify how vs the why of remote access.

The agency's security plan must document the "technical and administrative process" when remote access is enabled.

Virtual Escorting: All conditions must be met before allowing virtual escorting.

- Session shall be monitored at all times by an authorized escort
- Escort shall be familiar with the system/area where work is being performed
- Escort shall have the ability to terminate the session at any time
- Remote connections shall be encrypted using FIPS 140-2 certified encryption
- Remote admin personnel shall be identified prior to access and authenticated to or during the session

Policy Area 5.6.2.2

Requirements for user-based certificates

- When user-based certificates are used for authentication purposes, they shall:
- Be specific to an individual user and not to a particular device.
- Prohibit multiple users from utilizing the same certificate.
- Require the user to "activate" that certificate for each use in some manner (e.g. passphrase or user-specific PIIN).

Policy Area 5.10.1.2.2.b)

Encryption: New requirements that identify when encryption is not required for the transmission outside of the secure location.

- The agency owns, operates, manages, or protects the medium.
- Medium terminates within physically secure locations at both ends and no interconnections between.
- Physical access to the medium is controlled by the agency using the requirements in Sections 5.9.1 and 5.12.
- Protection includes safeguards and if feasible countermeasures to permit its use for the transmission of unencrypted information through an area of lesser classification or control.
- With prior approval of the CSO.

Policy Area 5.10.3.2

Virtualization: Several additional controls added for a virtualized environment. Please refer to the Policy if you deploy a virtualized environment.

Fast ID Fast Facts & Quarterly Update



WHAT IS *Fast ID*? *Fast ID* is an identification tool for law enforcement agencies only. It enables law enforcement officers to perform fingerprint searches from a roadside environment using a *Fast ID* mobile device.

**Fast ID BEGAN:
OCTOBER 6, 2011**

**# of Fast ID MOBILE
DEVICES IN MISSOURI:
143**

**# of Fast ID
SEARCHES SINCE
OCTOBER 6, 2011:
27,021**

**# of Fast ID
IDENTIFICATIONS
MADE SINCE
OCTOBER 6, 2011:
18,278 (68% ID RATE)**

**# of Fast ID
FBI RISC HITS SINCE
OCTOBER 6, 2011:
1,478**

Fast ID AGENCIES:

MSHP
Boone County SD
Columbia PD
St. Louis County PD
Gladstone PD
Velda City PD
St. Louis Metropolitan PD
St. Joseph PD
Sikeston PD
Florissant PD
Franklin County SD
St. Charles County PD
North Kansas City PD
Wentzville PD

Fast ID Q&A

HOW DOES *Fast ID* WORK? *Fast ID* is used to digitally scan the index fingers of an individual and submit the fingerprints for a two-finger comparison to the existing 2.8 million sets of fingerprints that are maintained in the state Automated Fingerprint Identification System (AFIS) at the Missouri State Highway Patrol (MSHP), which is the designated state Central Repository. The fingerprints are also forwarded on to the FBI for search against their Repository of Individuals of Special Concern (RISC), which contains approximately 2 - 3 million sets of fingerprints of sex offenders, known or suspected terrorists, immigration violators and federal fugitives.

WHAT INFORMATION IS RETURNED TO THE OFFICER AFTER A *Fast ID* SEARCH? The information returned on a *Fast ID* Search is limited. The state search returns the person's State Identification Number (SID), name, date of birth, sex and race. The FBI RISC search currently returns an FBI number along with which database was hit on, and with the implementation of the FBI's NGI Increment 4 on September 7, 2014, photos, when available, are also returned with RISC hits.

WHAT IS *Fast ID* USED FOR? *Fast ID* technology is used to identify people with no identification on them such as motorists with no drivers license, deceased persons, crime or disaster victims, persons with medical conditions (amnesia victims), etc..

IS THERE A COST FOR *Fast ID*? No. MSHP does not currently charge law enforcement agencies a fee to utilize this service at this time. Agencies are responsible for procurement of their own devices, as well as their connection to the MSHP.

WHAT INFORMATION IS STORED AFTER A *Fast ID* SEARCH? Only a transaction number is retained for statistical purposes only. No fingerprints are stored and no demographic information is sent, as the searches are 100% fingerprint-based.

ARE *Fast ID* SEARCHES SECURE? Yes. All *Fast ID* searches are conducted utilizing the existing secure connection between Missouri law enforcement agencies and the MSHP network. All RISC searches route through the secure MSHP/FBI CJIS WAN.

WHAT ARE THE BENEFITS OF *Fast ID*?

Officer Safety - Quick and Safe Method of Fingerprint-Based Identification

Public Safety - Enables officers to quickly identify threats to Missouri citizens

Public Service - Identifications that used to take hours now take seconds, resulting in better use of state resources and ultimately, tax dollars

*For more information about **Fast ID**, contact Jessica Mayhew, Program Supervisor, MSHP CJIS Division at (573) 526-6153 ext. 2787 or Jessica.Mayhew@mshp.dps.mo.gov*

LOG SCANS & OFFLINE SEARCHES

MSHP INFORMATION SECURITY UNIT

Phone: 573-522-3820

cjissecurity@mshp.dps.mo.gov



Log scans and offline searches are a special technique that the MSHP and NCIC can use to obtain information that is not available through an online query. The results may provide valuable investigative information for criminal and misuse cases or used as an administrative tool. For example:

Misuse

- Suspicion of an employee running information for unauthorized use
- Suspicion of an unauthorized person using an operator's credentials
- Suspicion of another agency running information for unauthorized use
- Improper dissemination

Administrative

- Needing to see a message that was deleted
- Checks of purged records
- In-house auditing

Criminal Investigation

An offline search of the MULES or NCIC transaction logs can reveal if a query was made on a particular individual or property item. This search could assist an officer in locating a property item, determining the proximity of an individual to a crime scene, substantiating or discrediting an alibi, or tracing the route of a person or vehicle of interest.

An offline search of the active MULES and NCIC databases can be run using one or more of the fields in the record. A use case for this search: a list of missing persons with an approximate age, race, sex, hair color, etc.

A search of all Criminal History transactions for a specific time frame. Some parameters of this search can include: ORI, FBI numbers, names, or social security numbers.

3 Solved Cases

Example 1 (transaction log search)

After identifying McVeigh as the renter of the explosives-laden Ryder truck, investigators requested an NCIC Offline Search on his name to be for all available information on him. An off-line search of NCIC's transaction log showed that about 90 minutes after the bombing, the Oklahoma State Highway Patrol made an inquiry on McVeigh. Armed with this information, investigators contacted the highway patrol and found that McVeigh was sitting—two days after the bombing—in a nearby jail cell on unrelated weapons charges.

Example 2 (active/purged record search)

In 2008, the FBI Chicago Field Office requested assistance identifying human remains found in a construction hole. The victim was killed execution style approximately 10 years earlier. A description of several tattoos obtained from the autopsy was searched through the database. A return of a missing person record identified the remains. The victim was the subject of a major La Cosa Nostra case. The investigators had long suspected that he had been murdered 10 years earlier during a drug deal that went bad, even though his body had not been found. (NCIC)

Example 3 (transaction log search)

On February 25, 2011, a 4-year-old child had been kidnapped by a noncustodial parent who had threatened to shoot the child and herself if law enforcement interfered. The U.S. Marshal in Pennsylvania working the case believed that the suspect was traveling to Florida. Using the New Jersey license plate of a vehicle associated with the suspect, the off-line search staff found an inquiry by a Utah law enforcement agency the previous week. The Marshals in Utah were able to locate the vehicle at the home of the suspect's sister where they placed a tracking device on the vehicle. The Marshals followed the vehicle to a gas station. When the subject when in to pay, the Marshal safely removed the child from the vehicle. The Marshal found a loaded gun in the car. The Marshal in Pennsylvania said that investigators had no indication that the suspect would be in Utah and would not have focused their efforts in that area without the results of the offline search.

Log Scan Portal

Located on the CJIS Launchpad in the CJIS Links section, the Log Scan Portal is a secure way to submit a request for a log scan or offline search. Personally identifiable information (PII) and criminal justice information (CJI) can be submitted through the portal. Please do not send PII and CJI in email format. All requests must be submitted through the secure portal. Please contact the MSHP ISU if you have any issues accessing the portal.

Search Results: If you have a department issued email address, the search results will be sent via email to the department email address. If the document contains CJI or PII, the document will be encrypted and password protected. If you do not have an agency email, the document will be encrypted and sent by mail to the agency.



Specific questions or concerns should be directed to the appropriate Division:

Information and Communication Technology Division

Call Center
1-800-877-2897
Email:
isdhelp@mshp.dps.mo.gov

Criminal Justice Information Services Division

UCR Unit
(573) 526-6278
Email:
ucr@mshp.dps.mo.gov

Access Integrity Unit
(573) 526-6141

CJIS Training Unit
(573) 526-6141

CJIS Audit Unit
(573) 526-6278

CJIS Information Security Unit
(573) 522-3820

AFIS, Quality Control, Sex Offender, CHS
(573) 526-6153

If you have a change in contact information, please contact the UCR Unit at the phone number listed above or CJISNews@mshp.dps.mo.gov

MULES

16-01

Missouri Uniform Law Enforcement System

File with MULES/NCIC Operations Manual

Person of Interest Entries (formerly STOP ORDERS)

When running a MULES inquiry on a subject, it is possible that an operator may receive a Person of Interest entry on their subject. Until recently these entries were called **Stop Orders**. While the name of the record has been changed, the methods for dealing with them have not. A Person of Interest is a MULES-only entry, meaning that it will always represent an entry made by another Missouri agency. There is no equivalent at this time in NCIC. Because the usual reaction to a matching MULES entry on a subject is enforcement action, it is important that all operators and officers understand how to handle Person of Interest records and the differences between these entries and Wanted, Missing, Protection Orders, etc.

The MULES Policy and Standards Manual states that a Person of Interest entry is used as a “notice that a person is wanted for questioning or a person of interest in a crime.” This entry is issued when an investigating officer has probable cause to believe a person has been involved in a crime, but is unable to obtain a warrant until further information can be derived from the individual. Person of Interest entries have no bond attached and automatically purge from the system after 1 year.

There are no policy requirements in place as to how an agency must handle this type of hit when received. It is encouraged that if the agency is within the extradition limits of the entry, a hit confirmation request is sent. This way, the entering agency can advise on how they wish to proceed. Inquiring officers and operators should always review these entries very carefully. Even though they are strongly encouraged not to do so, some agencies use Person of Interest entries for subjects who refuse to take their calls. These entries have been made in the past on witnesses to crimes and even victims of crimes. There are no requirements in place stating that an agency must hold, detain, or even take action on a Person of Interest entry. In fact, detaining or arresting a subject based solely on the existence of a Person of Interest entry is a violation of the subject of entry's civil rights.

In short, an operator or officer receiving a Person of Interest hit on a subject should first verify that the entry is of a criminal nature, and if so, follow the same steps followed when the subject of a criminal act message (such as a leave without pay) is contacted. Under no circumstances should the person be detained or placed under arrest based upon the Person of Interest hit alone.

A Person of Interest (Stop Order) Entry is . . .

- *Not a warrant*
- *Issued by an officer, not a court*
- *Based upon investigative information, not adjudicated*
- *Handled the same as a criminal act message*

Entering Protection Orders - Verifying information on the petition; relationships and Brady Indicator

Agencies responsible for verifying protection orders entered into MULES by a court should accept the order as soon as it is available in the VRFY queue. There should not be a policy of waiting until a paper copy of the order/petition is delivered to the agency. The purpose of the electronic transfer is to prevent delays in getting the order information into MULES/NCIC and waiting for paperwork defeats that purpose.

Still, when the associated paperwork is received, the order and petition should be reviewed to ensure that the information entered by the court is correct. In addition, there may be information available that it is not possible for the court to enter.

Petitioner's statement may include:

- Physical identifiers, such as tattoos, that are not found in the criminal history.
- Information that the person may be armed or violent

In addition, the operator should carefully review the narrative and verify that the relationship code is correct. Cases are regularly found in which the relationship that the court enters is incorrect, and therefore incorrectly sets the Brady Indicator.

The Brady Indicator denotes whether a person is prohibited from possessing firearms according to federal law, The Brady Handgun Violence Prevention Act.

The Brady Indicator is set automatically according to the codes used in the entry. It is not possible to "override" the Brady Indicator.

BRADY/Y indicates that the law applies to the respondent, and they may **NOT** possess a firearm.

BRADY/N indicates that the law does not apply, and the respondent may possess a firearm unless prohibited by judge's order (Protection Order Condition 07)

Three criteria are used to determine the Brady status

- Respondent must have had the opportunity to be heard (Brady will never be in effect for a temporary order)
- Relationship must be an "intimate" relationship
- Respondent presents a threat to petitioner, and is prohibited from using physical force against petitioner (Protection Order Condition 01)

The NCIC Operating Manual defines "Intimate Partner" as:

- With respect to a person, the spouse of the person, a former spouse of the person, an individual who is a parent of a child of the person, and an individual who cohabits or has cohabited with the person.

Cohabitation requires a live-in relationship (or former live-in relationship) between two individuals (can be same sex) which, in essence, is a sexual/romantic relationship, **NOT merely a roommate.**

...continued

Entering Protection Orders - Verifying information on the petition; relationships and Brady Indicator ...continued

Brady qualified relationship codes:

| | | |
|-------|-------------------------|---|
| CHCOM | Child-in-common | Parties are biological parents of the same child |
| CHILD | Child | Petitioner is the child of the respondent |
| EXSPS | Ex-spouse | Parties were formerly married |
| COHAB | Cohabiting Relationship | Parties were or are in a live-in romantic/sexual relationship |
| STCHD | Stepchild | Petitioner is the step child of the respondent |
| SPOUS | Spouse | Parties are married |

Non-qualified relationship codes:

| | | |
|------------------------------|----------------------|--|
| BGFRD | Boyfriend/Girlfriend | Parties are in a romantic/sexual relationship, but do not live together, nor have a child together |
| RMATE | Roommate | Parties live together, not in a relationship |
| RESID | Reside | Parties live together, not in a relationship |
| PARNT | Parent | Pet. is parent of the respondent |
| STPAR | Step Parent | Pet. is step parent of the respondent |
| All other codes are Brady/N. | | |

Common errors in entering the relationship

Most Brady errors are the result of a misunderstanding of the definition of the relationship codes.

For example, the relationship may be entered as BGFRD because the clerk/operator knows the parties do not live together; however they have a child in common. In this case, CHCOM would be the correct code.

Alternatively they may be entered as COHAB, if the subjects are dorm- or house-mates and not in a relationship. The appropriate code in this case would be RESID or RMATE.

...continued

Entering Protection Orders - Verifying information on the petition; relationships and Brady Indicator ...continued

| Brady "Yes" | Brady "No" |
|-------------|----------------------|
| COHAB | RESID |
| COHAB | RMATE |
| COHAB | BGFRD (non-residing) |
| CHCOM | BGFRD |

Though the court may initially enter the information in the electronic order, the entering/accepting agency is ultimately responsible for ensuring the accuracy and completeness of the entry. In addition to errors in the record quality aspect of a MULES audit, potential legal ramifications exist if a person is unjustly denied the ability to purchase a firearm, or if they are allowed to obtain one due to an entry error.

If repeated errors are discovered on the part of the court during entry of electronic orders, responsible agencies are encouraged to contact their court and provide them with the Brady guidelines. MULES trainers are also always happy to provide familiarization training to non-operators who may not be familiar with MULES/NCIC policies.

TAC Corner



Justice through Assured Knowledge and Enforcement Act - JAKE's Law **(Missouri Revised Statute 221.510.1)**

In February of 2000, six year old Jake Robel was killed after suspect Kim Davis stole the vehicle that he was sitting in. Jake's mother tried to remove him from the car as Davis drove away and Jake became tangled in the seatbelt. Jake was killed while hanging from the vehicle as Davis sped away at speeds over 70 miles per hour. Davis had just been released from a holding facility without a proper check for outstanding warrants. He was released from the facility, even though he had an active warrant in the system. JAKE's Law institutes the following rules and regulations to ensure a tragic mistake like this is not duplicated:

1. *All holding facilities, private or public is required to conduct a check for warrants within the MULES/NCIC databases on all prisoners about to be released, weather convicted of a crime or being held on suspicion of a crime*
2. *No prisoner can be transferred prior to a check run through MULES/NCIC*
3. *All holding facilities are required to notify the entering agency and cannot release the subject until the warrant has been dismissed, recalled or the entering agency has advised they do not wish to pursue the warrant to the current jurisdiction*
4. *All violations of Jake's Law are to be reported to the Missouri Attorney General's office*
5. *Direct violation of this law can result in a class A misdemeanor charge to the releasing individual*
6. *This law does not pertain to those records found outside the MULES and NCIC systems, such as REJIS-only records*

If a JAKE's Law check reveals an active warrant outside of extradition, the agency responsible for the record must still be notified and their extradition intent verified. This may be accomplished by sending an administrative message, or by using the JAKE's Law message template. A 'YQ' message can be used, but is not the optimal way to verify extradition intent in this situation. If no response is received from the entering agency, the inquiring agency can follow up with a phone call or secondary message if they deem it necessary. If you or your agency has any questions relating to a JAKE'S Law violation, please reach out to your district trainer or contact the Missouri Attorney General's Office.

Person with Information

Agencies with missing persons have the ability to utilize the Person with Information (PWI) entry in order to further efforts to locate a subject that has relevant information about an endangered or involuntary Missing Person that could assist or result in recovery. An example of where a Person with Information entry would be beneficial is a non-custodial parental abduction. Without this entry being in the system, any officer that might have contact with the noncustodial parent and child would not be alerted to the missing child by merely running the noncustodial parent. PWI entries require minimal information and are added to the missing person entry and can be used as long as certain criteria and rules are met, particularly in cases where the PWI is a parent, custodian, or legal guardian.

- Person with Information data may be appended to a Missing Person record entered using MKE/EME or EMI.
- Only the agency that entered the missing person record may append PWI data to that record. A Missing Person record may be appended with a maximum of two PWI records. Additional identifiers may be added to the PWI record as supplemental transactions.
- PWI data will require review 72 hours following entry and every 30 days thereafter.

RULES

- * When probable cause for arrest of the PWI nominee exists, a warrant must be obtained, entered and linked to the associated Missing Person record. If probable cause exists, but a warrant cannot be readily obtained, a Temporary Want should be entered into the Wanted Person File and linked to the Missing Person record.
- * If there is an active record in an unrelated matter in any person file for the PWI nominee, the record should be linked to the associated Missing Person record.
- * When none of the above are possible, the PWI capability may be used only when all of the conditions outlined below exist simultaneously.

CONDITIONS

Facts and circumstances indicate that:

- * The missing person was last seen under circumstances that pose a risk to the safety of that person.
- * There is a “substantial likelihood” that the PWI has relevant information about the missing person that could result in the recovery.
- * Entering identifying information concerning the PWI into the Missing Person record could assist the appropriate law enforcement agency to identify and interview the PWI, and that the resulting information could assist in the recovery of the missing person.
- * The PWI cannot be located and time is of the essence.
- * There is no prohibition under the investigating agency’s state law on the publication of information concerning the identity of a person for whom a warrant has not been obtained.
- * The identity of the PWI has been disclosed to the general public through an Amber Alert or other formal notification.

Once all the rules and conditions have been met the entry will be made using the EMP screen (Enter Person with Information) screen located in the Missing Person folder. This entry requires requestor information, NCIC #, Agency Case #, Name and miscellaneous information. All of the provided information is added to the NCIC missing person entry and will return a hit if the subjects name is queried. Since this information is added to the NCIC entry only it will only show up on the NCIC hit response and will not be reflected on the MULES entry.



Specific questions or concerns should be directed to the appropriate Division:

Information and Communication Technology Division

Call Center
1-800-877-2897
Email:
isdhelp@mshp.dps.mo.gov

Criminal Justice Information Services Division

UCR Unit
(573) 526-6278
Email:
ucr@mshp.dps.mo.gov

Access Integrity Unit
(573) 526-6141

CJIS Training Unit
(573) 526-6141

CJIS Audit Unit
(573) 526-6278

CJIS Information Security Unit
(573) 522-3820

AFIS, Quality Control, Sex Offender, CHS
(573) 526-6153

If you have a change in contact information, please contact the UCR Unit at the phone number listed above or CJISNews@mshp.dps.mo.gov

UCR

16-01

Uniform Crime Reporting

File with *Missouri Supplement to the UCR Handbook*

FBI UCR Transitioning to NIBRS-only Data Collection in 2021

The FBI National UCR Program staff worked with the CJIS Advisory Policy Board (APB) and with other national law enforcement organizations to fully support moving to a NIBRS-only collection at the national level. On February 9, 2016, FBI Director James B. Comey signed the following APB recommendation:

“The FBI UCR Program will transition to a NIBRS-only data collection by January 1, 2021, and will evaluate the probability of achieving that goal on an annual basis. Federal, state, local, and tribal agencies unable to meet the five year transition and who have committed to transitioning to NIBRS will collaborate with the FBI CJIS to develop a transition plan and timeline for conversion.”

Approximately 6,600 law enforcement agencies, representing 31 percent of the U.S. population, currently contribute crime data via NIBRS. Thirty-three states are certified to submit NIBRS data, 16 states submit only NIBRS data, and 17 states have some agencies that submit data via NIBRS and some agencies that submit data via the SRS. The national UCR Program staff are working diligently to engage and assist the state UCR Programs and U.S. territories that lack the capability to submit data via the NIBRS. Staff in the national UCR Program encourage local agencies, with approval from its state UCR Program, to contribute NIBRS data directly to the national UCR Program until the state UCR Program achieves NIBRS certification.

Efforts to transition agencies to NIBRS-only participation are underway with the assistance of the National Crime Statistics Exchange (NCS-X) Project, a collaboration between the national UCR Program and the Bureau of Justice Statistics (BJS). The NCS-X is not a separate data collection effort; rather, it is a strategic plan to increase the number of law enforcement agencies contributing NIBRS data so that NIBRS can generate statistically sound national estimates of crime.

Currently, the population served by many agencies that submit crime data via NIBRS is too small to make inferences about crime occurring at the national level. A valid statistical sample of 400 agencies, including the nation’s 72 largest agencies, was selected for participation in the NCS-X. When NIBRS data from these sampled agencies are added to the data from agencies currently submitting NIBRS data, the national UCR Program and BJS staff can accurately produce national estimates of crime. The staff from the national UCR Program and the NCS-X team are conducting outreach efforts that involve training, readiness assessments, educating the media and the public, assisting with planning and implementation strategies, and other measures that will ensure successful transitions to NIBRS-only reporting.

FBI UCR Transitions to NIBRS-only Reporting (continued)

In turn, please begin the process of reaching out to your records management system (RMS) vendor to determine if your agency is currently capable of submitting the required information to the MSHP. If not, what work is needed to ensure the system is NIBRS and MIBRS-compliant? We also recommend that you attend any of the POST-approved MIBRS Basic Training Classes held around the state in order to get a feel for the expanded data fields and much different workflow. Also, contact your local UCR Trainer/Auditor and schedule a meeting at your department to discuss your RMS, the MIBRS certification process, and your options. Finally, the MoUCR Program Staff is also available to speak to law enforcement executives, elected officials, local media, or special interest groups about UCR.

New Law Enforcement Use of Force Data Collection by FBI

Currently, the UCR Program collects the number of justifiable homicides reported by police as well as information about the felonious killings and assaults of law enforcement officers. These data are available in the annual *Crime in the United States (CIUS)* and *Law Enforcement Officers Killed and Assaulted (LEOKA)* publications. To provide an even broader picture of law enforcement incidents, the APB recommended, and Director Comey approved, the future collection and reporting of use-of-force incidents by law enforcement to the FBI. This includes use of force that results in the death or serious bodily injury of a person, as well as when a law enforcement officer discharges a firearm at or in the direction of a person. The national UCR Program defines “serious bodily injury” as “*bodily injury that involves a substantial risk of death, unconsciousness, protracted and obvious disfigurement, or protracted loss or impairment of the function of a bodily member, organ, or mental facility.*” This definition is based, in part, on the 18, *United States Code*, Section 2246 (4).

Further, the APB recommended, and Director Comey approved, the creation of a separate mechanism for the FBI CJIS Division to collect use-of-force-data. The national UCR Program will maintain the new data collection separately from the criminal incident and offense information, and it is working to build a collection management system for this purpose on the Law Enforcement Enterprise Portal (LEEP). The CSOs, in consultation with state UCR Program managers, will determine if agencies within their jurisdiction may submit use-of-force data directly to the FBI. State UCR Programs will have timely and ongoing access to all data submitted directly to the FBI.

Some FBI Use of Force data fields that have already been approved by the APB and the ongoing FBI Use of Force Task Force for collection are:

Age/Sex/Race/Ethnicity/Height/Weight of the Officer(s); Age/Sex/Race/Ethnicity/Height/Weight of the Subject(s); Date/time of the incident; NIBRS Location Code of Incident; Type(s) of Injury/Death of the Subject(s); Officer(s) injury type(s); Reason for initial contact between Subject and Officer; Did Subject resist arrest? Type of resistance/weapon involvement; Did Subject threaten force at Officer and/or another party?; Did Subject appear physically impaired? Was Subject armed or believed to be armed?; Type of Force used by officer to cause injury or death?

Reporting Assaults on Law Enforcement Officers in SRS & MIBRS

The LEOKA (Law Enforcement Officers Killed or Assaulted) is one of the most important and beneficial forms that an agency can report to the UCR Program. This form is the basis to begin formulating and implementing officer safety training. Therefore, it is very important that an agency accurately report and submit this data in a timely manner. Just like with reporting assaults on civilians, the same criteria to report the assault by weapon type is used to report LEOKA. The same rules apply when reporting assaults by hands, feet, fists as well. There is an exception when it comes to verbal intimidation directed towards a law enforcement officer.

In Summary Reporting, if a law enforcement officer is verbally assaulted without the use/display of a weapon or physical violence directed at the law enforcement officer, no assault for LEOKA would be reported. The FBI Summary Reporting User Manual V 1.0, page 148, states that “mere verbal abuse or minor resistance” is not reported as an assault for LEOKA and UCR purposes. If a weapon is used or displayed and/or physical violence is directed at the officer, then a LEOKA form would be completed by the agency.

For MIBRS agencies, an officer can be the victim of Intimidation-13C but the intimidation has to be more than “mere verbal abuse or minor resistance.” An example of intimidation for MIBRS would be were the suspect swings a fist or kicks at a law enforcement officer without making physical contact. Only personal weapons are used in an intimidation. If a weapon is used to threaten an officer, then an aggravated assault 13A would be reported. In MIBRS, no LEOKA form is submitted as the information is gathered from within the incident report from the following additional data elements: Type of Officer Activity/Circumstance (data element 25A), Officer Assignment Type (data element 25B), and Officer ORI (data element 25C).

If an agency ever needs assistance in determining if a LEOKA should be reported or how to report a LEOKA incident, please contact your regional UCR Trainer.

Reporting Drug Overdose Deaths in UCR

QUESTION:

An individual administers drugs to themselves and fatally overdoses. Could an agency report a Manslaughter by Negligence for the person who gave/sold the drugs to the victim?

ANSWER:

For NIBRS and SRS agencies: If someone takes drugs of his/her own free will and overdoses, the national UCR Program considers this an accidental death, regardless of any charges lodged by the agency. The only exception would be is if police determine that someone had intentionally laced the drug with a substance meant to kill, in which case, the National Program would consider the incident to be a criminal homicide.

New NIBRS/MIBRS Offenses

The Advisory Policy Board made the recommendation to add two new Fraud offenses to NIBRS. FBI Director James Comey signed off on the implementation for the addition of Fraud - Identity Theft, 26F and Fraud - Computer Hacking, 26G. Both offenses became active January 1, 2016. This implementation does not affect those submitting Summary data.

Fraud - Identity Theft, 26F: *“Wrongfully obtaining and using another person’s personal data (e.g., name, date of birth, Social Security number, driver’s license number, credit card number).”*

Fraud - Computer Hacking, 26G: *“Wrongfully gaining access to another person’s or institution’s computer software, hardware, or networks without authorized permissions or security clearances.”*

The MIBRS Specification Manual has been updated and is available under the downloads tab of the MoUCR Homepage.

Animal Cruelty

For NIBRS/MIBRS agencies, a new Group A offense of “Animal Cruelty” has been implemented. The FBI will collect this data starting with the January 2016 calendar year. The following is the FBI’s national definition for Animal Cruelty: *“Intentionally, knowingly, or recklessly taking an action that mistreats or kills any animal without just cause, such as torturing, tormenting, mutilation, maiming, poisoning, or abandonment. Included are instances of duty to provide care, e.g., shelter, food, water, care if sick or injured; transporting or confining an animal in a manner likely to cause injury or death; causing an animal to fight with another; inflicting excessive or repeated unnecessary pain or suffering, e.g., uses objects to beat or torture an animal. This definition does not include proper maintenance of animals for show or sport; use of animals for food, lawful hunting, fishing, or trapping.”*

As with most Group A offenses, there is certain data elements that must be completed. Under Data Element 12 (Type Criminal Activity/Gang Information) the agency must select one of the four types of abuse. These are listed below with their associated NIBRS code:

- A = Simple/Gross Neglect (failure to provide food, water, shelter, veterinary care, or intentionally or knowingly withholding food or water)
- I = Intentional Abuse and Torture
- F = Organized Abuse (dog fighting and cock fighting)
- S = Animal Sexual Abuse (bestiality)

The MIBRS Specification Manual has been updated and is available under the download tab of the MoUCR Homepage.

Classifying and Scoring Assaults

One of the most common errors encountered by the CJIS Auditors is the over-reporting of Aggravated Assaults by Hands, Feet, Fists. The most common reason for this error is due to an agency's over-reliance on their records management system (RMS) when producing their UCR. In the real world, when an officer enters a report on an assault where the victim was assault by personal weapons, they selected the first assault or UCR code that shows "hands, feet, fists" when coding the report for UCR. Or the agency's RMS is hard coded to the offense table incorrectly. Either of these situations can drastically affect an agency's overall crime rate. In one recent study conducted by an auditor, it was found that 72% of the Aggravated Assaults by Hands, Feet, Fists reported by 8 agencies were over-reported. These 8 agencies initially reported a combined total of 158 aggravated assaults by hands, feet, fists. Upon review, 113 were found to be over-reported. These 113 aggravated assaults should have been reported as simple assaults. The Missouri Uniform Crime Reporting Program recommends that the agency use one or more of the following steps to ensure accurate reporting of assaults.

1.) When an agency produces their monthly UCR, the reports that are coded to the UCR as Aggravated Assaults by Hands, Feet, Fists should be reviewed to ensure accurate reported. A good rule of thumb is when the agency has more aggravated assaults by hands, feet, fists, than Other Assaults-Simple to report for a month, there is a strong possibility that some of those aggravated assaults are over reported.

2.) The agency should use the UCR audit report, details reported, report generated or whatever the agency's RMS generates for UCR to check those offense reports that a listed as aggravated assaults by hands, feet, fists. Depending on the RMS an agency has, this report may only list the aggravated assault by hands, feet, fists as a number taken from the Return A. The most common numbers used by RMS for aggravated assaults, hands, feet, fists, are 4D or 44.

3.) If the agency's UCR offense table and offense code tables are hard coded to set the UCR by selection of the offense, be sure that these codes are linked correctly or the UCR code for that selected offense can be changed in the individual report.

4.) Finally and most importantly, use the Federal Bureau of Investigation's National UCR Standard Offense Definitions when reporting. *"The category Aggravated Assault—Hands, Fists, Feet, etc.—Aggravated Injury (4d) includes only the attacks using personal weapons such as hands, arms, feet, fists, and teeth, that result in serious or aggravated injury. Reporting agencies are to consider the seriousness of the injury as the primary factor in establishing whether the assault is aggravated or simple. The assault is aggravated if the personal injury is serious, for example, there are broken bones, internal injuries, or stitches required. Conversely, the offense is considered simple assault if the injuries are not serious (abrasions, minor lacerations, or contusions) and require no more than usual first-aid treatment."* (Emphasis added) FBI Summary Reporting System (SRS) Users Manual, V 1.0, page 39-40

If any agency needs guidance or has questions relating to classification of any UCR offense, please contact your regional UCR trainer. Training is also available for officers/deputies as well as those that produce an agency's Uniform Crime Reports.

Changes In LEOKA Reporting

LEOKA stands for Law Enforcement Officer Killed or Assaulted. This form gathers minimal information on officers killed or assaulted in the line of duty. Information gathered from this form is used as the basis to start the process of implementing officer safety training. Therefore, this form is one of most important forms that an agency can submit. It is very important that an agency accurately report and submit this data in a timely manner.

To qualify as a law enforcement officer for LEOKA, the officer/deputy had to meet the following criteria:

- ◇Wear/carry a badge (ordinarily)
- ◇Carry a firearm (ordinarily)
- ◇Be duly sworn and have full arrest powers
- ◇Be a member of a public governmental law enforcement agency and be paid from government funds set aside specifically for payment to sworn law enforcement
- ◇Be acting in official capacity, whether on or off duty, at the time of the incident
- ◇Deaths which are directly related to the injuries received during the incident

Effective 03/23/2016, the FBI has expanded who would qualify to have LEOKA reported. These exceptions are:

- ◇Individuals who are killed or assaulted while as a law enforcement officer at the request of a law enforcement agency whose officer meet the current collection criteria
- ◇Special circumstances will be reviewed by LEOKA staff on a case-by-case basis to determine inclusion
- ◇Includes military and civilian police and law enforcement officers of the Department of Defense, while performing a law enforcement function/duty who are not in a combat or deployed status

Deaths resulting from the following are not included in the LEOKA program's statistics:

- ◇Natural causes such as heart attack, stroke, aneurism, etc.
- ◇On duty but death is attributed to personal situations such as lover's quarrel/triangle, neighbor conflict, etc.
- ◇Suicide

The following are examples of job positions not included in LEOKA statistics:

- ◇Corrections/correctional officers/jailers
- ◇Bailiffs
- ◇Parole/probation officers
- ◇Judges
- ◇U.S and Assistant U.S. Attorneys
- ◇Prosecutors
- ◇Bureau of Prison officers

If your agency needs assistance with reporting a LEOKA incident, please contact your regional UCR Trainer.

Reporting Related Crimes Occurring in Multiple Jurisdictions

QUESTION:

Checks were stolen from residences in one location (Jurisdiction A) and were then used at banks and grocery stores in another location (Jurisdiction B). Should law enforcement personnel in Jurisdiction A report the crimes of forgery and uttering or should Jurisdiction B report the crimes?

ANSWERS:

For NIBRS agencies: For UCR reporting purposes, agencies should report only crimes that occur in their jurisdiction, and crimes should be reported in the most local jurisdiction. In the above example, the agency in Jurisdiction A should report the theft of the checks (through robbery, burglary, purse snatching, etc.), and the staff in Jurisdiction B should report the forgery and fraud.

For SRS agencies: If the checks were taken during a robbery, burglary, larceny-theft, etc., in Jurisdiction A, then the law enforcement agency from Jurisdiction A should report that offense. If the individual was then arrested in Jurisdiction B for using the stolen checks, staff from Jurisdiction B should report the arrest for forgery and fraud on the appropriate Age, Sex, Race, and Ethnicity of Persons Arrested report.

2017 Change to LEOKA Incident Date/Time Requirements for NIBRS

Currently, law enforcement agencies entering information into Data Element 3 (Incident Date/Hour) via NIBRS include the month, day, year, and hour that an incident occurred, started, or the beginning of the time period in which it occurred. Data Element 3 (Incident Date/Hour) is a mandatory data element, but if the incident hour is unknown, it is left **blank**.

Beginning on January 1, 2017, when an agency reports a murder or nonnegligent manslaughter (offense code 09A), an aggravated assault (offense code 13A), a simple assault (offense code 13B), or an intimidation (offense code 13C) and the victim is a law enforcement officer, the agency must report the incident hour.

If the hour is left blank, the agency will receive the following error message:

When Data Element 25 (Type of Victim) = L (Law Enforcement Officer) then Data Element 3 (Incident Date/Hour) must be populated with a valid hour (00-23). Incident Hour Unknown (Blank) is not a valid entry.

National UCR Program staff will update NIBRS documentation to reflect this change. Staff made this decision because of the recent attention involving officer-involved incidents in addition to the importance and value of having complete data in the LEOKA Program.

All Missouri L.E. Agencies are invited to attend the 2016 ASUCRP Conference!

September 26-29, 2016

The Hotel Alyeska

Girdwood, Alaska

www.alyeskaresort.com



The Alaska Department of Public Safety is hosting the 2016 Association of State Uniform Crime Reporting Programs (ASUCRP) National Conference. This preeminent crime statistics conference will again feature the most up-to-date information from the leading subject matter experts. Such topics will include the sunset of the Summary Reporting System, the nationwide transition to NIBRS, the status of the National Crime Statistics Exchange Project (NCS-X), the White House Police Data Initiative, the details and timeframes for new Use of Force reporting, and extra training on Animal Cruelty, Human Trafficking, Cargo Theft, and Identity Theft reporting. Speakers from the Federal Bureau of Investigation's (FBI) UCR Program Office, the FBI Crime Data Modernization Team, the CJIS Advisory Policy Board (APB), the CJIS APB's UCR Subcommittee, the Bureau of Justice Statistics (BJS), the Bureau of Indian Affairs (BIA), the IJIS Institute, SEARCH, and many current UCR Program Managers will discuss upcoming changes to the FBI's UCR Quality Assurance Review (QAR) process, creation of public UCR dashboards, examine media use/misuse of crime statistics, share tips for new State UCR Program Managers, and explain the new XML-based data format and associated NIBRS IEPD.

All state, county, local, campus, railroad and tribal law enforcement agencies, as well as analysts, academics, and special interest groups, are welcome to attend. Please visit the below link for registration forms, a tentative agenda, an area activity guide, and hotel information:

<http://asucrp.net/conferences/2016-asucrp-conference/>



Missouri State

Highway Patrol

