Missouri State Highway Patrol
Criminal Justice Information Services Division

The CJIS Newsletter

MHP
Issue 25-1
March, 2025

Information in this newsletter is considered MULES policy and may rescind information that is currently shown in the MULES Manual and other state level policy publications until those publications can be updated. Please ensure that all CJIS systems operators at your agency review this newsletter.

Missouri CJIS Staff

CJIS Systems Officer:

Major Christopher Jolly

CJIS Division Director

Captain Gara Howard

CJIS Division Assistant Director

Kerry Creach
Operations Section

CJIS Division Assistant Director

Tim Schlueter
Technical Systems/Training & Auditing Section

CJIS Division Assistant Director

Steve White
Cyber Security & Technology Section

CJIS Division Assistant Director

J.D. Reece
Application Development & Support Section

CJIS Division Assistant Director

Valerie Hampton
Administrative Support Section

CJIS Welcomes New Troop A MULES Trainer, Sherry Clark!

We're very excited to introduce Sherry Clark as our new Troop A MULES Trainer. Sherry brings over 25 years of experience in dispatch and enforcement to the position having held positions with Jasper County Sheriff's Office, Missouri Department of Liquor Control, Joplin Police Department and the Federal Reserve Bank in Kansas City.

Sherry will be working in the coming weeks to familiarize herself with the agencies in Troop A, scheduling additional classes for the last half of 2025, and get settled in the position. Along with that, she joins us just in time to assist with the move of Troop A Headquarters to their new location at 1900 Northeast Independence Avenue in Lee's Summit!

Sherry can be reached by phone at (816) 622-0707 ext. 3135 or by email at sherry.clark@mshp.dps.mo.gov.

Welcome Sherry!

Inside this issue:

The CJIS Newsletter

MHP

Issue 25-1

March, 2025

Missouri Sex Offender Registry Conference 2025 Registration Now Open!

The Missouri State Trooper's Association is hosting the 2025 Sex Offender Registry Conference, sponsored by Huber & Associates. The primary goal of the conference is to unite agencies in our shared mission to track and manage sex offenders required to register. To assist in this mission, the Criminal Justice Information Services Division will facilitate conversations and update stakeholders on the policies and procedures regarding Missouri Sex Offender Registration laws and the Sex Offender Registration and Notification Act (SORNA). Presentations will cover a range of topics, which include information on the Revised Statutes of Missouri (RSMo), caselaw updates, Sex Offender Registration policies and procedures, Department Of Corrections (DOC) electronic monitoring, SOR system entry and overview, a demonstration of the new Missouri Sex Offender Registry System (MoSOR), and a variety of other insightful presentations.

The conference is designed to be inclusive of criminal justice agencies with a vested interest in the Missouri Sex Offender Registration process. POST credit hours will be offered to sworn law enforcement personnel. Continuing Legal Education (CLE's) will be offered to licensed individuals with the Missouri Bar. Don't miss out on this opportunity to unite and gain valuable insight to the latest policies, procedures, techniques, and laws affecting various levels of the criminal justice system.

Registration information can be found on the Missouri State Troopers' Association website, MissouriTrooper.com under "Public Events" on the main page.

Date: August 19-21, 2025
Location: The Resort at Lake of the Ozarks
3076 Bagnell Dam Blvd
Lake Ozark, MO 65049

Hotel information can be found on the MOSTA registration website.

Hope to see you there!

The CJIS Newsletter

MHP

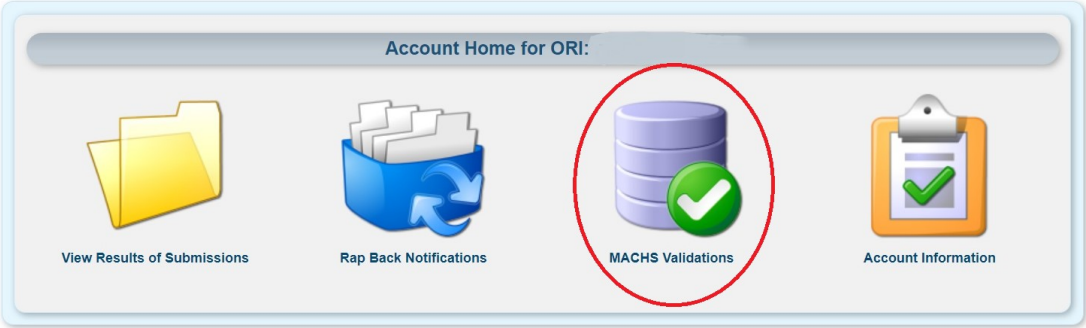
Issue 25-1

March, 2025

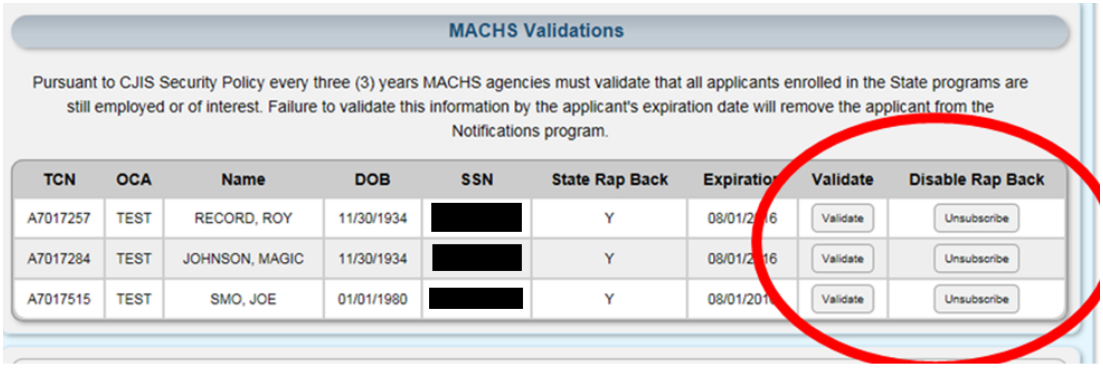
RAP Back Validations

Dan Yepsen, Troop D MULES Trainer

People with MACHS access for RAP Back may have noticed emails in the last few months about validations. This is because RAP Back subscriptions are required to be validated every three years, and it has been roughly three years since RAP Back became a requirement for sworn officers. Whenever a validation is due, MACHS users will receive an email approximately 35 months after an individual is fingerprinted for RAP Back enrollment. The MACHS Admin must then log into MACHS and complete the validation before the end of the 36th month after the individual was fingerprinted. For example: if an individual is enrolled into RAP Back on 4/16/22, they will be able to be validated on 3/1/25. The agency then has until 4/30/25 to complete the validation. If the individual is not validated, they will be automatically unsubscribed from RAP Back. When it is time to do a validation, the MACHS Admin can log in to MACHS and click on the MACHS Validations icon.



They will then see the queue of pending validations. The MACHS Admin will review the list and click on Validate if the individual is still under their purview, or Unsubscribe if they are not. Please note that failing to unsubscribe an individual no longer under their purview can open an agency up to liability should a RAP Back hit occur and they view the RAP Sheet.



A second, optional way for an agency with a large number of enrolled individuals to validate is the Batch Validation. The MACHS Admin can click on the Download button to obtain a tab-delimited text file containing a list of all individuals due for validation. Then simply remove the row for any record(s) that should no longer be active, save the file, and upload it back into MACHS. MACHS will then validate every record on the list. Any record that was removed from the file will stay in the queue and can be unsubscribed at that point, or wait until the end of the period to be automatically unsubscribed.

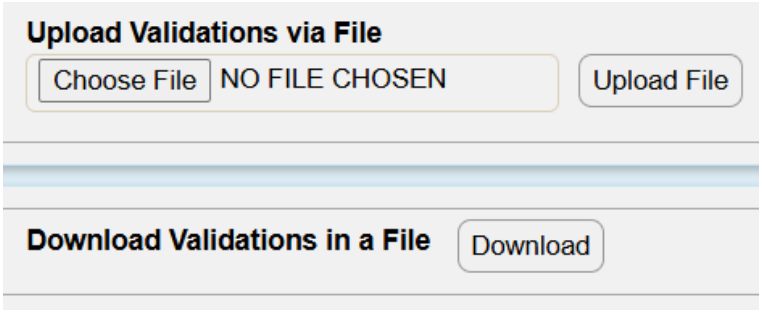
(Continued on Next Page)

The CJIS Newsletter

MHP

Issue 25-1

March, 2025



Here are a couple of other quick tips and reminders for RAP Back:

- Once an individual is unsubscribed, whether that be from an agency unsubscribing when they leave, or by failing to validate the subscription every three years, the only way to get someone resubscribed is to fingerprint them again
- If your agency also utilizes a Z ORI for CCWs, make sure individuals are fingerprinted using the correct ORI, and that MACHS users login with the correct ORI to check on a status, complete validations, to unsubscribe, etc
- MACHS only retains the fingerprint response for 90 days before it expires. You can ask your MULES Trainer about a MACHS Retention form which will keep the responses indefinitely
- Agencies must have a signed Applicant Privacy Notice document for all individuals currently in RAP Back. This can kept as a paper copy or digitally
- Per CJIS Security Policy, any MACHS users who do not log into MACHS for longer than 90 days may have their MACHS access removed. MACHS access would then need to be requested for the user again through the MULES User Portal by selecting MACHS ORI Admin or MACHS ORI Read Only

Violent Person Files Records Loaded

Chris Parr, CJIS Program Manager

The CJIS IT Section recently finished loading 75,908 records into the NCIC Violent Person File. These records represent the subjects with qualifying Missouri convictions for entry criteria 2 and 3. This brings the total of subjects entered based on conviction data to over 86,000. Agencies can expect to start seeing these records on query responses and are reminded that they are informational only. No enforcement action should be taken based on these records alone and they should not be confirmed.

Criminal justice agencies are also reminded that criteria 4 is available for subjects who have expressed intent to harm any criminal justice personnel. This includes police officers, probation officers, judges, prosecutors, dispatchers, etc. The NCIC Violent Person File is viewable nation wide and provides vital officer safety information.

See the flyer on the next page for more information and call your MULES trainer with any questions.

CAUTION

Threat to law enforcement

NCIC Violent Persons File (VPF)

Persons who have been convicted of violence against a police officer	***Persons who have expressed an intent of violence against a police officer***	***Automatically searched with an NCIC WANTED PERSONS QUERY (QW)***
ALERT	**ALERT**	**ALERT**

The VPF is designed to alert law enforcement officers that the individual they are encountering may have the propensity for violence against law enforcement.

Description

An entry into the VPF should be made when at least one of the Violent Person Criteria (VPC) has been met:

1. **The offender has been convicted of assault or murder/homicide of a law enforcement officer, fleeing, resisting arrest, or any such statute which involves violence against law enforcement.**

2. **The offender has been convicted of a violent offense against a person, including homicide and attempted homicide.**

3. **The offender has been convicted of a violent offense against a person in which a firearm or weapon was used.**

4. **A law enforcement agency, based on its official investigatory duties, reasonably believes that the individual has seriously expressed his or her intent to commit an act of unlawful violence against a member of the law enforcement or criminal justice community.**

The CJIS Newsletter

MHP

Issue 25-1

March, 2025

SOR Forms Updated

The Sex Offender Registry registration form, SHP-428, signature page has been updated to be inclusive of Missouri Revised Statutes 589.426, 566.150 and 566.155. The SOR system will automatically generate the new version upon registration. If your agency uses hard copy forms, the new version can be found on the CJIS Launchpad. The SOR Unit can also provide the new forms upon request.

Additionally, the Address Verification Letter has been updated. The letters aim to be direct with clear instructions.

Out of State Withdrawals on Missouri DOR Response

Deirdre Carter, Troop F & I MULES Trainer

You may have noticed more information returning on some Missouri driver license responses, even more than the typical long response you have been seeing since November. These are violations the driver has received in other states, shared via the Driver's License Compact (DLC). This information displays below the issuance and medical certification information.

```
OUT OF STATE WITHDRAWAL INFORMATION:
1) TYPE/I - INFORMATIONAL              AAMVA WITHDRAWAL              STATE/SC
     EFFECTIVE/12 26 2008 LOCATOR #/111111111  031
     WDW TYPE/SUSPENDED        BASIS/1 - CONVICTION
     EXTENT/ALL              APPEAL/NOT DEFINED
     ELIG REIN/   ACTU REIN/12 26 2012 REFERENCE/013
2) TYPE/I - INFORMATIONAL              AAMVA WITHDRAWAL              STATE/SC
     EFFECTIVE/12 25 2007 LOCATOR #/111111111  029
     WDW TYPE/SUSPENDED        BASIS/1 - CONVICTION
     EXTENT/ALL              APPEAL/NOT DEFINED
     ELIG REIN/   ACTU REIN/12 12 2012 REFERENCE/013
3) TYPE/I - INFORMATIONAL              AAMVA WITHDRAWAL              STATE/SC
     EFFECTIVE/12 21 2000 LOCATOR #/111111111  004
     WDW TYPE/SUSPENDED        BASIS/1 - CONVICTION
     EXTENT/ALL              APPEAL/NOT DEFINED
     ELIG REIN/   ACTU REIN/12 11 2012 REFERENCE/013
```

The Driver's License Compact is an agreement between 45 U.S. states to share information about driver's license violations and suspensions. The compact aims to enhance highway safety, ensure that drivers meet the same standards across state lines, and streamline the process of handling out-of-state traffic violations.

Under the DLC, when a driver commits a traffic offense in a member state, that state reports the violation to the driver's home state. This allows the home state to apply penalties, such as points on the driver's record, even if the offense occurred in another state. It also means that a suspension or revocation in one state can affect the driver's ability to hold a license in their home state.

If you have any questions, please reach out to your MULES trainer.

The CJIS Newsletter

MHP

Issue 25-1

March, 2025

Cargo Theft in NIBRS

Scott Cline, Troop I and G Auditor

Cargo theft is defined by the FBI as theft of an item between the manufacturer and either the individual business, or other shipping company. Once it reaches its destination, it is no longer in the supply chain. So, once the package is delivered to the mailbox/front porch/etc, it is no longer considered Cargo Theft.

Data Element 2A (Cargo Theft)

Data Element 2A indicates whether or not the incident involved a cargo theft. The National UCR Program has defined Cargo Theft as "the criminal taking of any cargo including, but not limited to, goods, chattels, money, or baggage that constitutes, in whole or in part, a commercial shipment of freight moving in commerce, from any pipeline system, railroad car, motor truck, or other vehicle, or from any tank or storage facility, station house, platform, or depot, or from any vessel or wharf, or from any aircraft, air terminal, airport, aircraft terminal or air freight station, warehouse, freight distribution facility, or freight consolidation facility. For purposes of this definition, cargo shall be deemed as moving in commerce at all points between the point of origin and the final destination, regardless of any temporary stop while awaiting transshipment or otherwise."

Two key phrases in the classification of cargo theft are "commercial shipment" and "in the supply chain." For LEAs to classify an incident as a cargo theft, the items must be part of a commercial shipment and must be in the supply chain (i.e., moving in commerce). LEAs should consider thefts from United Parcel Service (UPS), Federal Express (FedEx), the U.S. Postal Service, etc., to be cargo until the items arrive at a final distribution point. Once the business receives the items (i.e., personnel at the company sign for the goods), the goods are no longer considered cargo because they are outside of the supply chain. **Therefore, LEAs should not consider deliveries from UPS, FedEx, to individuals or other businesses (e.g., flowers, pizza, electronics, appliances, etc.) to be cargo because they are outside of the supply chain.**

Examples:

If you order a new uniform from 5.11 Tactical, once 5.11 gives the item to UPS/FedEx/USPS for delivery, and the uniform is stolen from their delivery truck, it is out of the supply chain and not considered Cargo Theft.

If you order a new belt/holster from Amazon and someone steals the package from your doorstep. This is considered outside of the supply chain as it has been delivered to its final destination and is not considered Cargo Theft.

MULES Manual Update

Each January the MULES Manual is updated with all of the Technical and Operational Updates (TOUs) from the previous year. The update for 2025 is complete and all updates can now be found in the Manual.

It's important to remember this newsletter is a policy document and changes and updates to policy are posted here first, before they're added to the Manual. Don't forget to check the CJIS Newsletter for up to date policy when questions come up.

The CJIS Newsletter

MHP

Issue 25-1

March, 2025

SACU and You: Everything you never wanted to know about the CJIS Security Policy

Scott Robinson, CJIS Program Coordinator

Bottom Line Up Front (BLUF): The CJIS Security Policy (CJISSECPOL), version 6.0, was released on December 27, 2024. This version completes the modernization process, and all updates/modernization are complete. Modernization changes are not limited to just a few areas but affect the entire policy and the way agencies who process/store/utilize criminal justice information do business. Compliance requirements have been divided into Priority 1, 2, 3, and 4 categories. Agencies should focus on Priority 1 requirements as these are designed to be the most significant and impactful compliance requirements to protect each agencies network. The Patrol will schedule and conduct trainings sessions across the state to better prepare agencies for the expanded compliance requirements.

To prepare agencies for the additional compliance requirements in the new CJIS Security Policy (CJISSECPOL), the Security Audit and Compliance Unit (SACU), have posted specific policy templates and compliance documents on the CJIS Launchpad. These templates and compliance documents are broken down by the policy section to allow agencies to focus on specific areas to ensure compliance. Current efforts should be directed towards Priority 1 compliance requirements, which are broken out by priority levels in the compliance documents. The Patrol is currently planning training sessions to take place later in the year. There will be morning and afternoon training sessions offered. During the session each section of the policy is discussed and focuses on compliance requirements. Watch for future announcements on this training.

Additionally, as the Patrol further understands and refines the compliance requirements we will share this information with all agencies. Supply Chain Risk Management requires agencies to be aware of potential vulnerabilities inherent in applications and hardware purchased from vendors. To meet this requirement the Patrol is implementing the below to facilitate compliance with this section of the CJISSECPOL:

CJIS Security Policy Version 6.0 incorporates Supply Chain Risk Management. Under this section an agency is required to have:

1. A supply chain/acquisition policy,

2. An individual with overall responsibility to manage supply chain risk

3. Establish a supply chain management team that involves the organization's procurement process such as IT, purchasing, legal, and other relevant entities to ensure compliance with supply chain management.

4. Follow procurement methods that use preferred vendors who can provide attestation or compliance with state and federal standards. Missouri currently follows federal standards that can be found here:
   A. https://www.fcc.gov/supplychain/coveredlist
   B. https://vsc.gsa.gov/drupal/node/6

5. Ensure that vendors are required through purchasing agreements to notify the agency when there are patches, updates, exploits or breaches of the vendor that may cause risk to CJI

6. Ensure that upon acceptance of systems or system components, the agency inspects the product(s) for tampering and periodically inspects the systems for tampering

(continued on next page)

7. Ensure that disposal of systems occurs such that any CJI is protected based upon the Media Protection policy, i.e. – delete or destroy.

The Security Audit and Compliance Unit is actively coordinating with the FBI CJIS Division Audit Team to understand the changes and how each will impact Missouri agencies. This is a learning process for each of us and, in advance, I appreciate everyone's patience as we, collectively, work through the changes to maintain compliance with the CJISSECPOL.
If you have questions about policy compliance requirements, please reach out to SACU via the email: securityaudit@mshp.dps.mo.gov.

Fixing NIBRS Errors and Warnings

Kevin Neeley, Troop A Metro Auditor

Anything that shows on the NIBRS Errors and Warnings dropdown needs to be looked at to either be correct, deleted, or verified (which then would be hidden on the site).

Errors:
Agency corrects Incident in their RMS and re-uploads onto a new file.
Agency corrects Incident using Incident Editor. Make sure your RMS shows the same data.
Agency submits an Incident deletion onto a new file.
Agency submits an Incident deletion using Incident Editor.

Warnings:
Agency can verify the Warning by providing details about the Incident to their local MSHP Trainer/Auditor. Then it will be hidden on the site by the MSHP Trainer/Auditor.

* If the Incident is ever uploaded again with modifications, the Warning may come back. *

Agency corrects Incident in their RMS and re-uploads onto a new file.
Agency corrects Incident using Incident Editor. Make sure your RMS shows the same data.
Agency submits an Incident deletion onto a new file.
Agency submits an Incident deletion using Incident Editor.

We Want Your Violent Person File Success Stories!

Have you had an encounter recently with a subject entered in the NCIC Violent Person File where the information in the entry helped avoid an officer safety incident? Or have you had good results based off of entering a subject into the NCIC Violent Person File? Help spread knowledge and awareness of the Violent Person File with your success stories! Email the details to Christopher.parr@mshp.dps.mo.gov, and we may share them in this newsletter and with NCIC for national recognition!

CYBERSECURITY

Upcoming Training

Protecting CJI During Critical Events: Cyber-Resiliency and CJIS Security Policy Compliance

March 26-27 | 7 a.m. – 4 p.m.

As law enforcement agencies become increasingly targeted by cybercriminals, protecting sensitive information and upholding the foundations of justice have never been more critical. Join us for this important Criminal Justice Information (CJI) security awareness training covering all critical security requirements and standards.

Topics:

- Current threat landscape for criminal justice agencies
- Computer intrusion case study
- Cybersecurity in the cloud - risks and strategies for protection
- Compliance:
  - Risk assessments
  - Criminal Justice Information Services (CJIS) compliancy - new policies as of December 27, 2024
  - Tabletop exercises
- Tools and resources available to assist with compliance

Target Audience:

- Criminal justice agencies including law enforcement, corrections, probation and parole and prosecutors
- Agency CIOs and CSOs
- Individuals supporting information technology at criminal justice agencies
- IT staff (i.e., professionals working with network infrastructure, hardware, etc.)
- Law enforcement leadership staff

Presented by:

Police KC/MO

Register>>

Register online at
https://shorturl.at/RBO5q

SCAN ME

Cost

FREE TO ATTEND

Location

KCPD Regional Police Academy
6885 N.E. Pleasant Valley Rd
KCMO 64119

Contact:

For more information, please contact Jackie Chapman-Fagan
Jackie.ChapmanFagan@kcpd.org

MARC
MID-AMERICA REGIONAL COUNCIL

The Mid-America Regional Council is the nonprofit association of local governments and the metropolitan planning organization for the bistate Kansas City region.

The CJIS Newsletter

MHP

Issue 25-1

March, 2025

Purpose Code C vs. Purpose Code F

Mike Zvolanek, Troop H & B MULES Trainer

When running a firearm related criminal history transaction, a user may wonder which purpose code they should be using. Obviously, it depends on the origin of the request. Is it a criminal investigation or a firearm related background check? The answer to that question will determine if you use purpose code **C** or **F**.

Purpose code C, as defined by the III/NFF Manual, would be used in the following situations:

"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."

This would include criminal investigations that involve firearms. This is not an all-inclusive list, but some examples would include assault, homicide, possession, and theft.

To define purpose code F, we will again refer to the III/NFF Manual which states it is used for weapons related background checks. The manual states it would be used in the following situations:

"(a) issue firearms-related permits and explosives permits pursuant to state law, regulation, or local ordinance; (b) return firearms to their lawful owners; and (c) enforce federal and state laws prohibiting certain persons with criminal records from possessing firearms in circumstances in which firearms have been pawned."

So from this we can see that use of purpose code F is limited to checks for concealed carry permits or other licenses or to check a subject before returning seized or recovered firearms to their rightful owners. In this case the initial check would be via the National Instant Criminal Background Check System (NICS) using a numeric purpose code and if the results are inconclusive, a full RAP sheet can be requested using the RAP Sheet transaction (QMH) and purpose code F. It should be noted that the NICS Check (QNP) can only be used when issuing a weapon related permit or returning a weapon from LE custody back to the owner. In those cases, the NICS check should be run instead of a standard criminal history query so disqualifiers aren't missed.

The next time you run a firearm related criminal history transaction, simply ask yourself, "is this related to a criminal investigation, or is this related to a weapon related background check?" If the answer is a criminal investigation, use purpose code C in your transaction. If the answer is weapons related background check, use purpose code F.

The Nlets Administrative Message Information Sharing Initiative

Who are we?

The National Threat Operations Section (NTOS) is located at the Criminal Justice Information Service (CJIS) Division in Clarksburg, WV. The NTOS mission is to protect the nation by serving as the primary communication channel through which the public provides information pertaining to federal criminal violations and threats to national security.

Why are you getting Nlets Administrative Messages from NTOS?

In alignment with the CJIS Advisory Policy Board and in support of the FBI's mission to equip our state and local partners with the criminal justice information they need to fulfill their mission of keeping communities safe, NTOS began providing state and local tip information directly to respective agencies via International Public Safety and Justice Network (Nlets) Administrative Messages (AMs) on 06/01/2023. These messages contain information that does not rise to a federal investigation level but may be related to your agency's law enforcement functions. NTOS does not require any action. Your agency determines how to use the information.

What does the Nlets message look like?

TITLE: FBI NATIONAL THREAT OPERATIONS CENTER INFORMATION SHARING

CAVEAT: THE INFORMATION HEREIN WAS SUBMITTED BY THE PUBLIC, SOCIAL MEDIA OR PRIVATE SECTOR COMPANIES TO THE FBI TIP LINE AND HAS NOT BEEN CONFIRMED, INVESTIGATED, OR VETTED BY THE FBI. THE INFORMATION PROVIDED IS TO BE USED AT THE DISCRETION OF THE RECEIVING AGENCY TO FURTHER ITS LAW ENFORCEMENT FUNCTIONS. THIS MAY INCLUDE JUVENILE-RELATED INFORMATION, MEANING EACH RECEIVING LAW ENFORCEMENT AGENCY MUST UTILIZE IT SOLELY BASED ON THEIR INVESTIGATIVE NECESSITY. YOU ARE RECEIVING THIS MESSAGE BASED ON ZIP CODE MAPPING.

ORI RECIPIENTS: 12345A, 67890B

OTHER RELEVANT ACTION: TEST PSAP CONTACTED

TRANSACTION REFERENCE NUMBER: 12345XYZ

SYNOPSIS: TEST

What can you do with the messages?

Since the messages are informational in nature, NTOS does not require any action. However, below are some examples of how agencies can use the information received:

- Open new investigations in your area
- Aid current investigations
- Provide awareness for officer safety

CONTACT US WITH ANY QUESTIONS

NTOS Information Sharing Team - NTOS_LIAISON@FBI.GOV

Missouri CJIS System Officer – Diane Bartell, phone: 651-793-2590, email: diane.bartell@state.mn.us

Date Last Modified: 12/30/

UNCLASSIFIED

The CJIS Newsletter

MHP

Issue 25-1

March, 2025

Use of Unknown Bias Type in NIBRS

Kevin Neeley, Troop A Metro Auditor

Many officers/deputies will use the MIBRS Bias Type of 99=Unknown when there is no indication of a bias type in the incident. This is incorrect usage of 99=Unknown. As of 01/15/2025, there are 2,985 unresolved warnings due to the use of 99=Unknown. These are published as Hate Crimes, and the data is accessible to the general public. Below is a report from the public page of MSHP Show Me Crime statistical web page. This is why it is very important that these warnings are resolved.

NIBRS Crimes and Rates by County -
Last 3 Years
Current date: 1/15/2025 8:11:57 AM (Central Standard Time)
Data source: MO_SS, Offense Data

Bias Motivation	Unknown (offender's motivation not known)			
Measures	Number of Crimes			
Incident Date	2025	2024	2023	
Jurisdiction by Geography				
Missouri	1	738	693	

https://showmecrime.mo.gov/public/View/dispview.aspx

99=Unknown is to only be used when there is evidence that the incident was bias motivated, but it is unsure what the bias type is. The majority of offenses in an incident should have the Bias Type of 88=None reported. If through the investigation it is learned that the incident was bias motivated, then the Bias Type can be changed to the actual bias type and resubmitted.

New Platform for Livescan Devices

Andrew Benner, CJIS Program Coordinator

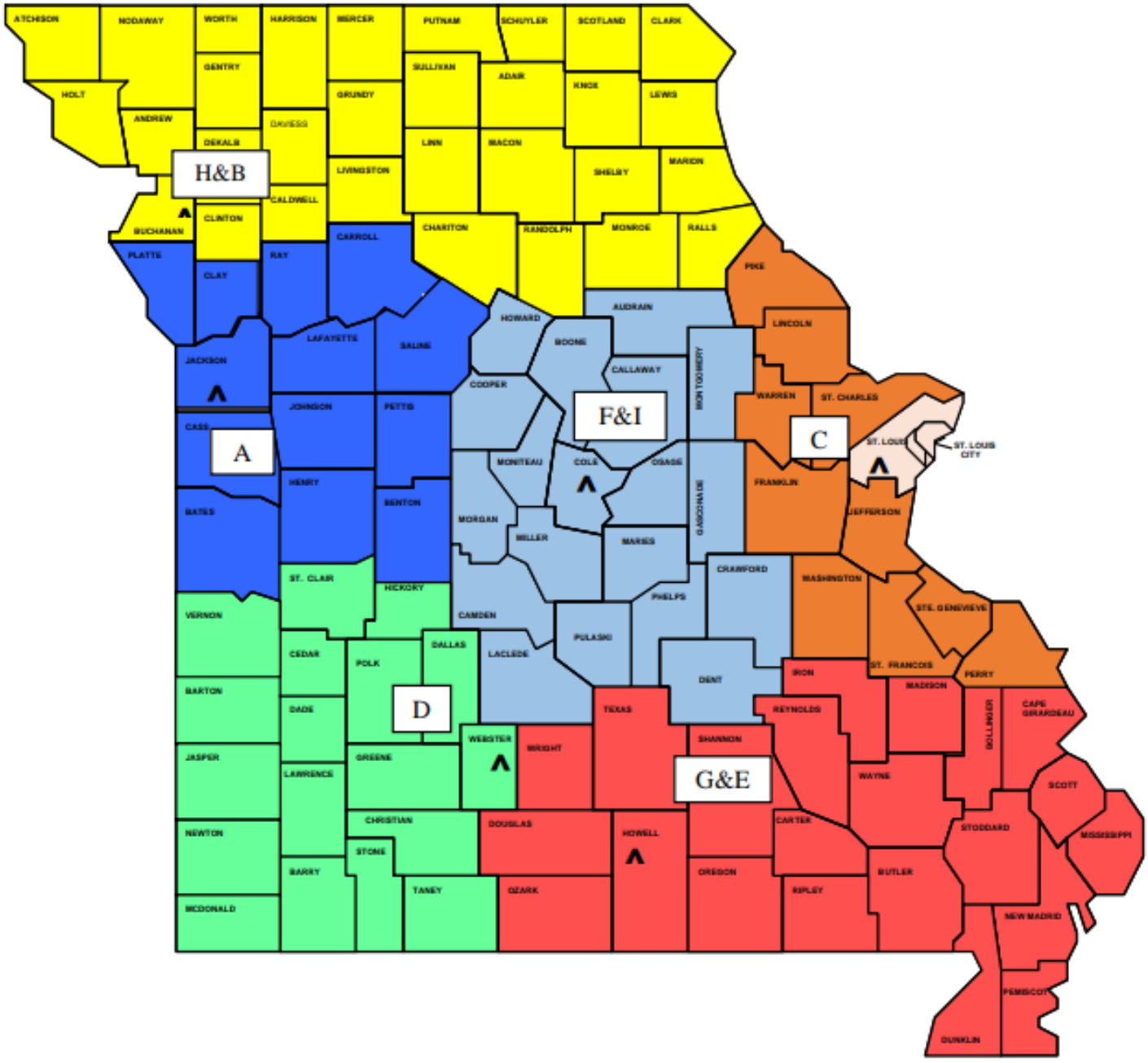
In June 2019, Idemia ended technical support for the ILS2 livescan platform. At that time, the software stopped receiving feature enhancements, security patches and any other fixes or support. Due to the outdated operating system and lack of security enhancements, ILS livescans which are livescans that were installed prior to 2014, can no longer connect to the MSHP Network. MSHP compiled and reviewed all known ILS devices and contacted affected agencies. If you believe you have an ILS device please contact Andrew Benner, 573-526-6264 or Andrew.Benner@mshp.dps.mo.gov.

In January 2025 Idemia ended technical support for the ELSA livescan platform. While these devices will continue to function, they will no longer receive feature enhancements, security patches or other fixes. ELSA livescans which are livescans installed between 2014 and 2022 can still utilize the MSHP Network. There are no immediate requirements to remove these devices. But agencies should be aware as security requirements evolve, ELSA devices will eventually need to be removed from the network as well.

The most current livescan platform is TPE, with over 200 devices deployed throughout the state. TPE devices, livescans installed in 2022 or later, will continue to receive feature enhancements, security patches, and support.

MULES Training Unit

Troop Contact Information



Troop A Trainer	Sherry Clark	816-622-0707 x3135	sherry.clark@mshp.dps.mo.gov
Troop B & H Trainer	Mike Zvolanek	816-387-2344 x3859	michael.zvolanek@mshp.dps.mo.gov
Troop C Metro Trainer	Bruce Snider	636-300-2800 x3355	bruce.snider@mshp.dps.mo.gov
Troop C Rural Trainer	Trevor Dunn	636-300-2800 x3355	trevor.dunn@mshp.dps.mo.gov
Troop D Trainer	Daniel Yepsen	417-895-6868 x6409	daniel.yepsen@mshp.dps.mo.gov
Troop G & E Trainer	Sam Tuck	417-469-3121 x3762	sam.tuck@mshp.dps.mo.gov
Troop F & I Trainer	Deirdre Carter	573-751-1000 x3621	deirdre.carter@mshp.dps.mo.gov
Unit Supervisor	Chris Parr	573-526-7189	christopher.parr@mshp.dps.mo.gov