Utah Department of Public Safety

Dissemination, Misuse, & RMS

BCI Field Services
2025 TAC Conference

Dissemination

Dissemination

Dissemination is the act of spreading or circulating information. The act of dissemination with regards to UCJIS information is associated with (i) a User disseminating information to another User, and (ii) a User disseminating information to recipient agencies. Criminal justice personnel must understand that all information acquired through UCJIS is protected. Discussing UCJIS information with non-criminal justice personnel is against federal laws and Utah Code 53-10-108.

Verbal

Radio, Scanner, Phone, In-person

Electronic

Email, Fax

Printed

Printouts from UCJIS

Dissemination Rules

The Basics

- Who can I disseminate UCJIS information to?
  - Authorized personnel who have a legitimate need to know

- Who can I NOT disseminate UCJIS information to?
  - City Mayor
  - City Council Member
  - Legislators
  - Civilians

- Consider the following questions before disseminating:
  - Do they have authorization?
  - Why do they need this information?
  - What is my agency's policy/procedure?

Dissemination Rules

User Disseminating Information to Another User

- Can disseminate between Users and Non-Access Users within your agency if-
  - The person is authorized to receive such information; and
  - It’s for criminal justice purposes

- Not necessary to keep a separate log of this transaction
  - UCJIS maintains the dissemination log of transactions for you

Dissemination Rules

Secondary Dissemination

- Can disseminate to another criminal justice agency if-
  - The agency is an authorized recipient of such information; and
  - It’s for criminal justice purposes

Dissemination Rules

Secondary Dissemination

- When partaking in secondary dissemination-
  - A secondary dissemination log must be kept; and
  - The agency providing CJIS data must train the recipient agency on dissemination, privacy, and security of CJIS data

Secondary Dissemination Logs

Used whenever sharing information between authorized agencies. Must track the who, what, when, and why.

Secondary Dissemination Logs

Date of dissemination	What was released	Recipient Agency	Person CJIS was released to	Number associated with request
5/1/2025	Criminal History: Bear, Yogi	NYPD	Joseph Test	202512345
5/17/2025	III: Mouse, Mickey	Metro PD	Joseph Test	202554321
7/4/2025	Driver's License: Possible, Kim	Zootopia PD	Whitney Wilson	202579657
7/30/2025	Criminal History: Duck, Donald	BCI	Dylan Cane	202535978

Dissemination Rules

Juvenile Records

- Juvenile records cannot be disseminated
  - Not allowed to print out a hard copy of a juvenile's rap sheet/record summary or cut and paste anything per the Juvenile Courts
    - You may, however, allude to or summarize this information

- Juvenile records cannot be accessed for ROA purposes

- Juveniles wanting a copy of their record need to be sent to the Courts
  - Same goes for any individuals that come in and request a Court record or disposition information

Misuse

Misuse

Misuse is to use something in the wrong way or for the wrong purpose. Misuse of the UCJIS system applies (whether you are set up as a User, Non-Access User, or Non-User). Misuse can also happen if you are not set up in UCJIS at all. Possible repercussions of misuse include criminal/civil charges, termination of employment, loss of UCJIS access, loss of POST certification, etc.

UCA 53-10-108

It is a Class B Misdemeanor for a person to knowingly or intentionally access, use, disclose, or disseminate a record created, maintained, or to which access is granted by the division or any information contained in a record created, maintained, or to which access is granted by the division for a purpose prohibited or not permitted by statute, rule, regulation, or policy of a governmental entity.

Misuse Rules

- UCJIS can only be accessed for criminal justice related purposes
  - No curiosity checks or personal inquiries
    - I.e., running partner to see if they have a warrant

- No matter which device is used, dissemination, privacy, and security laws governing misuse of UCJIS information still apply

- Do not use the license plate number of friends, neighbors, co-workers, etc., for training/testing purposes, including on UCJIS Test

Misuse Rules
Continued

- Familiarize yourself with your agency's misuse policy
  - Includes UCA 53-10-108 and potential repercussions

- Misuse Statute is included on User/Non-User agreements-

User/Non-User Security Agreement

Misuse of UCJIS information: Violation of dissemination, privacy, or security regulations may result in civil and/or criminal prosecution of the person(s) involved and loss of state computer access for the user and his/her agency. BCI maintains an automated dissemination log of all UCJIS file transactions to help ensure this information is being accessed for authorized purposes. Any unauthorized request or receipt of this information could be considered misuse. Utah Code Annotated 53-10-108(12) (a) states:

(12) (a) It is a class B misdemeanor for a person to knowingly or intentionally access, use, disclose, or disseminate a record created, maintained, or to which access is granted by BCI or any information contained in a record created, maintained, or to which access is granted by BCI for a purpose prohibited or not permitted by statute, rule, regulation, or policy of a governmental entity.

User/Non-Access User Training & Testing Agreement

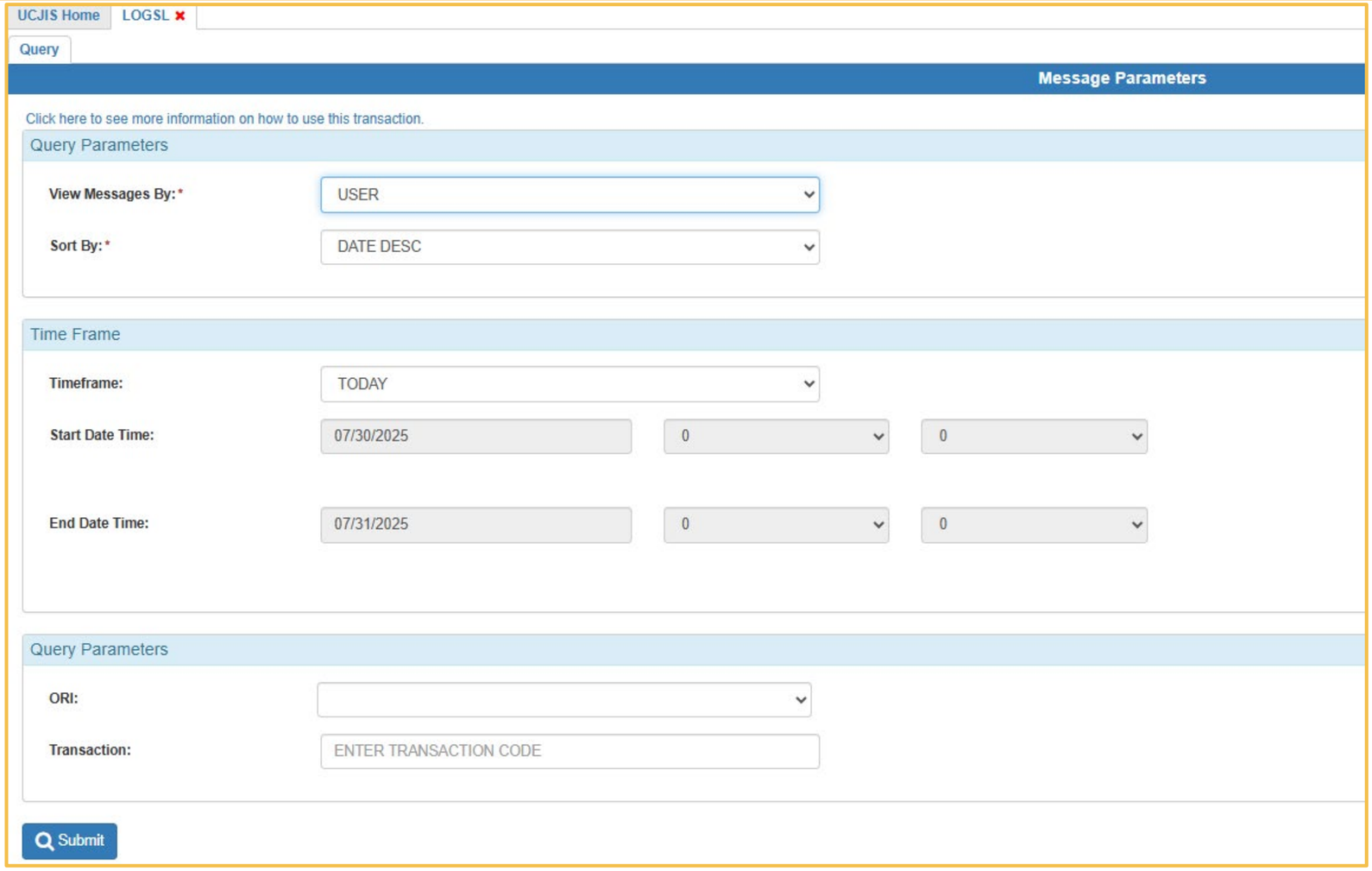
UCJIS USER AND NON-ACCESS USER AGREEMENT

I certify that by signing this document that I have been trained and/or proficiency tested according to the procedure set by my agency, BCI, and CJIS. I accept that I will be held accountable for any information accessed under my user ID. I understand per **Utah Code Annotated 53-10-108 (12)(a),** it is a class B misdemeanor for a person to knowingly or intentionally access, use, disclose, or disseminate a record created, maintained, or to which access is granted by BCI or any information contained in a record created, maintained, or to which access is granted by BCI for a purpose prohibited or not permitted by statute, rule, regulation, or policy of a governmental entity.

LOGS Transaction

Each time a User requests/enters information into UCJIS, UCJIS ‘disseminates’ information to the User. A log of the transaction is created by the system for security and liability purposes. This log records the date and time, user ID of person making the request, file accessed, and the search criteria.

LOGS Transaction



LOGS Transaction

Audit Log Results
Created by alarson on 04/26/2024 09:06:43

Received Time	Agency	UserID	Transaction	ORI	Search Fields
04/25/2024 16:37	BCIFS	OVAISIMA	CHQ	UT	SID=701580;PURPOSE_CODE=C;REQUESTER=OVAISIMA;AUDIT_REASON=TEST YOGI BEAR
04/25/2024 16:37	BCIFS	OVAISIMA	CHQ	UT	SID=321323;PURPOSE_CODE=C;REQUESTER=OVAISIMA;AUDIT_REASON=TEST YOGI BEAR
04/25/2024 16:28	BCIFS	ADOUGLAS	QV	UT	NIC=
04/25/2024 16:28	BCIFS	ADOUGLAS	QW	UT	
04/25/2024 15:21	BCIFS	OVAISIMA	CHQ	UT	SID=701580;PURPOSE_CODE=C;REQUESTER=OVAISIMA;AUDIT_REASON=TEST YOGI BEAR
04/25/2024 14:29	BCIFS	JHARR	QSW	UT	COURT_ID= ;CASE_NUMBER=
04/25/2024 14:28	BCIFS	JHARR	QSW	UT	COURT_ID= ;CASE_NUMBER=
04/25/2024 14:28	BCIFS	JHARR	QSW	UT	COURT_ID= ;CASE_NUMBER=
04/25/2024 14:28	BCIFS	JHARR	QSW	UT	COURT_ID= ;CASE_NUMBER=
04/25/2024 14:27	BCIFS	JHARR	QSW	UT	COURT_ID= ;CASE_NUMBER=

Misuse Rules

LOGS Transaction

- All transactions in UCJIS are logged
  - BCI and the FBI can see the who, what, when, and why behind searches

- TAC/Alt TACs must be checking their LOGS regularly to ensure misuse is detected in a timely manner
  - Can view all transactions ran by Users within the past 21 days

- We've seen an increase in misuse/dissemination cases not being found right away because LOGS aren't being checked regularly
  - Make sure you check your LOGS at least once a week

How is Misuse Found?

- TAC's weekly review of the LOGS transaction
- BCI audits
- FBI audits
- Self-reporting
  - Anyone who becomes aware of misuse must inform their agency, the Commissioner, and the BCI Director per UCA 53-10-108(12)(b)

Misuse Cases & Outcomes

- Officer accessed Nlets information to set up a traffic stop for his fiancée's ex-husband, resulting in the man's car being towed and impounded.
  - Charged with six misdemeanors

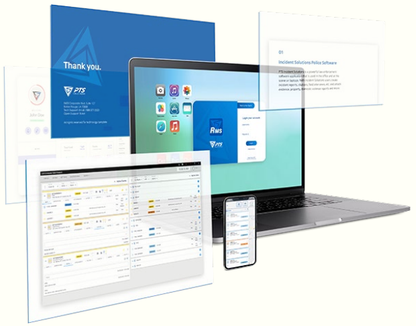
- Officer ran their teenager's information to see if they had a traffic ticket.
  - Disciplined by department

- UCJIS User also worked a part time job unrelated to the criminal justice field. They were helping a customer that only had a digital ID and ran them to verify the ID was valid, but this wasn't for criminal justice nor a case with the agency.
  - Disciplined by department

RMS

RMS

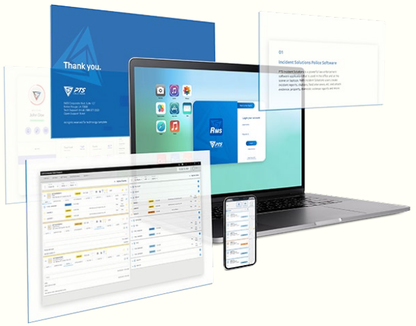
RMS stands for a Record Management System. This is a secure database which stores UCJIS information and is usually used by Law Enforcement Agencies for dispatch and record storage purposes. For example, your agency may use an RMS such as Spillman or Fatpot to store agency case files. Because the RMS stores UCJIS information, it is required to meet CJIS standards and policies.



RMS Rules

- Anyone with direct RMS access must be set up properly under that agency's ORI
  - Must be at least a Non-Access User
  - Can't be a Non-User
    - Unless there's blockers in place to prevent Non-Users from coming across CJI within RMS

- Who doesn't qualify for RMS access?
  - Any person or agency that doesn't have proper UCJIS access and authorization to receive the information
    - City Officials
    - Fire Departments
    - Volunteers

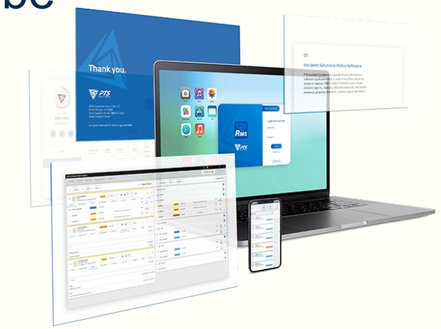


RMS Rules *Continued*

- All information acquired through UCJIS is protected
  - Whether you access it through an RMS or UCJIS directly- same rules apply

- Accessing RMS for personal reasons is considered misuse
  - Reviewing reports not part of your caseload for someone you know
  - Pulling up Court and PD files to stalk someone

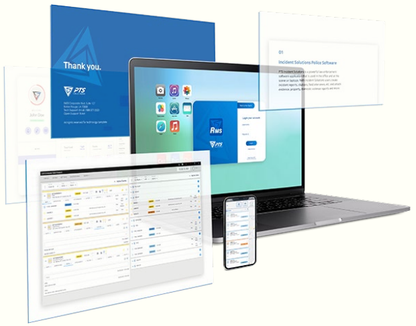
- If you share a county-wide RMS system, access needs to be restricted



RMS Rules *Continued*

- What can be stored in the RMS?
  - Case files
    - Screenshots of NCIC entries
    - Broadcast messages
    - Driver’s License photos

- What cannot be stored in the RMS?
  - Juvenile records
  - Driver’s License photos for future photo lineups
    - Contact SIAC to have those retrieved for you



Knowledge Check

All information acquired through UCJIS is protected

True

False

What UCJIS type should an RMS User be?

User

Non-Access User

Non-User

Dissemination can be verbal, electronic, or printed

True

False

UCJIS can be used for curiosity checks

Yes

No

What is the Misuse Statute?

UCA 53-10-108

Scenarios

Scenario #1

A local Animal Control agency has access to Utah Driver's License and DMV information, but nothing else. They ask Zootopia PD to run a potential wanted person in NCIC and provide that information to them. Should Zootopia PD fulfill this request?

No. Just because Zootopia PD has access to NCIC, it doesn't mean they can run something on there and provide it to another agency. The local Animal Control agency is not authorized to access or receive NCIC information, therefore, fulfilling this request would be considered unauthorized dissemination and misuse.

Scenario #2

Trooper Tom has a potential suspect pulled over on the side of the road and calls up dispatch to run a background check on him. Dispatch runs the information and finds the suspect has several outstanding warrants. Can dispatch share this with Trooper Tom? Does a secondary dissemination log need to be kept to track this?

Yes. This is fine as long as Trooper Tom has a valid reason to know that information. A dissemination log is not required to be kept in this case because dispatch is acting on behalf of the agency.

Scenario #3

Kim Possible works for a Criminal Justice Agency (CJA) but doesn't have access to III. She knows her coworker, Rufus, is set up under the CJA with access to the file and wants him to run a III record and provide that information back to her. Can Rufus fulfill Kim's request?

No. If someone works for the same CJA as you, but doesn't have access (to III for example), you can't run that information and provide it to them. This would be unauthorized dissemination.

Scenario #4

An officer took a screenshot from their RMS system, which was reflecting UCJIS information, and then posted it on social media as a public service announcement. Is this okay?

No. Although the individual may have had good intentions, the public is not allowed to receive such information from UCJIS. This would be considered unauthorized dissemination and, therefore, misuse.

Scenario #5

A Fire Department requests their local PD run background checks on some of their new employees and provide them with the results. Can the local PD fulfill this request despite the Fire Department not being set up as a CJA?

Not unless it is done through an ROA. Otherwise, the dissemination wouldn't be authorized because the Fire Department is not properly set up and authorized to receive such information.

Scenario #6

A Medical Examiner's Office is conducting a death investigation and requests the full investigation file on the deceased individual from Law Enforcement. Can the LEA provide this information to them?

Yes, the LEA can provide this to them with a few restrictions. The investigative file may be shared for their death investigation, excluding criminal history. The LEA must redact the criminal history prior to sharing the investigation file with the Medical Examiner's Office.

[UCA 63G-2-206]

Scenario #7

While entering the arrest information from incoming citations, you notice a citation came in for your coworker's daughter. Can you tell your coworker about this?

No, dissemination of this information, even within the department, is not authorized in this situation and would be considered misuse. There needs to be a valid criminal justice purpose for the dissemination.

Scenario #8

An authorized Attorney's Office requests the Sheriff’s Office disseminate a jail inmate’s fingerprint card to them for the purpose of enhancing charges. The fingerprint card shows the state ID number and FBI number. Can the Sheriff’s Office provide this to them?

Yes, the Sheriff’s Office can provide this to them because it’s for an authorized purpose and being shared with an authorized recipient.

Scenario #9

A User joins a virtual meeting with their camera on. Their other monitors are visible showing UCJIS information pulled up. Those in attendance are able to see the User viewing a criminal history through CHQ. Is this allowed?

No, this is not allowed. The User should not be sharing a screen showing such information to everyone in the meeting.

Scenario #10

The Police Chief requests you run the Medical Marijuana transaction (MMJL) as part of a new hire background check and disseminate your findings to them. Is this allowed?

No, this is not allowed. MMJL can only be run to verify the validity of someone's Medical Cannabis Card for the administration of criminal justice. It cannot be used for criminal justice employment purposes.

[UCA 26B-4-202]

Scenario #11

A local CJA is requested to disseminate a Juvenile record for the purpose of a Presentence Investigation (PSI). Is this considered misuse?

Yes, if the Juvenile history came from the Courts, there is a prohibition on printing that information. What juvenile information is obtained in UCJIS also comes directly from the Courts so the same rules apply. You cannot copy and paste anything directly but you can allude to or summarize that information for the probable cause.

Scenario #12

A local PD wants to include a Driver's License (DL) photo within the case file on RMS that's linked to that specific person for their investigation. Is this allowed?

Yes, this is fine because it is part of the investigation.

[18 USC § 2721]

Please Remember

- Make sure your people are set up properly on your ORI to receive information if applicable
- Check LOGS transaction regularly to look for misuse
- Portable devices accessing UCJIS information fall under the same dissemination, privacy, security and misuse regulations as a desktop computer located in a locked office
- Do not run things for another User or agency that doesn’t have that access

FAQ

Q: Are we required to keep a dissemination log when running ROA's for the public?
A: Yes, a secondary dissemination log must be kept when disseminating ROA's to the public/requestor.

Q: How do we find out if another agency is authorized to receive information?
A: Generally, you'll know if they have a valid ORI or are part of your process. You can also contact Field Services.

Q: Can we electronically disseminate juvenile drivers license information to defense councils?
A: You need to consult the juvenile court and/or your attorney for this question.

FAQ

Q: Can you email criminal history in a downloaded file to an officer if asked?
A: As long as the criminal history is sent securely through email encryption.

Q: Can an ROA be ran for a juvenile who is almost 18 for them to start college?
A: If it’s through the official ROA process, then yes you can run them, but UCH is the only UCJIS file that can be searched and it only contains adult criminal histories so a rap sheet wouldn’t be returned. The Utah Juvenile Criminal History file must never be accessed for ROA purposes.

THANK YOU!

BCI Field Services
2025 TAC Conference