Dissemination Basics

TAC Conference 2022

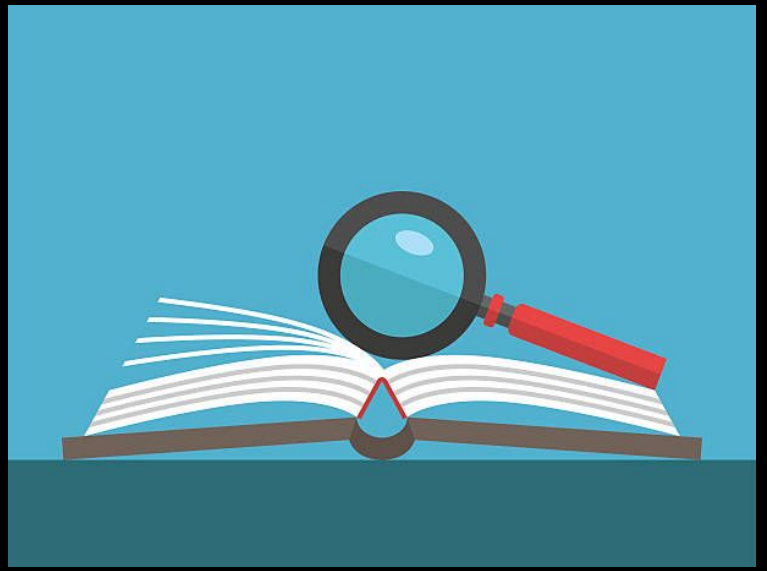
What does it mean to disseminate information?

dis·sem·i·nate

/dəˈsemə¸nāt/

verb

1. Spread (something, especially information) widely.

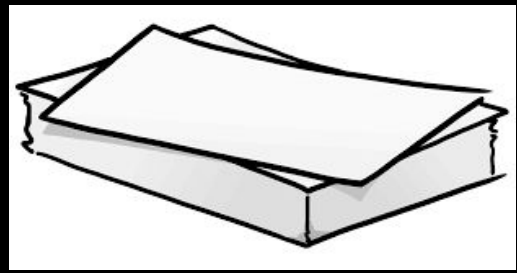


UCJIS Basics 4.0

Dissemination is the act of spreading or circulating information. Criminal justice personnel must understand that all information acquired through UCJIS is protected.

Types of Dissemination

- Electronic
- Verbal
- Printed



Who is the first point of contact?

Agency Users

Agency Users are the individuals that are considered the first point of contact because they are logging into the system directly

U S E R

Any individual that has unescorted access to UCJIS information or UCJIS terminals

N O N - A C E S S U S E R

Receives and uses UCJIS information,

but does not log directly into UCJIS

NON-USER

No UCJIS access

Dissemination Within Your Agency

- User
- Non- Access User
- Non User

Transaction LOGS

- Date / Time
- Agency ORI
- User ID
- Transaction
- Information Accessed

Dissemination Logs

LOGS Transaction: TAC’s must periodically run the LOGS transaction to see what transactions users are running and to assist in the protection for your agency from misuse

TAC’s can view all transactions ran by users within the past twenty one days only

Can I give UCJIS Information to another agency?

Consider the following questions before disseminating:

- Do they have authorization?
- Why do they need this information?
- What is my agency's policy/procedure?

Dissemination of information from UCJIS

All information acquired from any file accessed in UCJIS is governed by regulations and policies of the FBI and State of Utah

Dissemination of any information acquired from any file in UCJIS should be for Criminal Justice Purposes (unless given via an ROA)

Secondary Dissemination

If an agency provides any information from UCJIS to another criminal justice agency or for Motion of Discovery purposes, it is considered secondary dissemination

Servicing Agency vs. Recipient Agency

When a servicing agency releases information from UCJIS to another agency(recipient agency), a Secondary Dissemination log must be maintained at the servicing agency

If the servicing agency wishes, they may request that the recipient agency sign a UCJIS Information Exchange Agreement before information may be provided to the recipient agency

Secondary Dissemination Log

The log must include the date of the dissemination, the name of the recipient agency, the name of the person the information was released to, and the case name/number related to the release.

Recipient agencies are only authorized to have this information for criminal justice purposes.

UCJIS Access

UCJIS is a web-based system that is being accessed from many different devices. This includes mobile devices such as smartphones, tablets, laptops, etc.

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

Destruction of Information

Destroy all media stored with criminal justice information.

Paper destruction

- Cross Cut Shred

Working Remotely

Working Remotely

Many agencies have asked if it is possible to access CJIS/UCJIS systems and data remotely. The FBI has provided the document below to help answer many of the questions regarding remote access and ensuring compliance with CJIS policies and best practices. Please reach out to your Field Services Representative with any additional questions you have.

Maintaining CJIS Compliance While Working Remotely Download

Working Remotely

Agencies should review their policies to see under which scenarios working from home is appropriate and which positions are authorized

Reporting security incidents for unauthorized access to CJI including unauthorized transfer of CJI to a non agency device should be included

Unauthorized individuals (family members, roommates, ect.) are not permitted to view CJI or operate devices that contain or can access CJIS

Creating A Controlled Area

Remote employees must designate areas where CJIS is stored or processes as a controlled area to properly protect CJIS

In a home environment, individuals must take necessary precautions to protect the information from not being disseminated to anyone who should not have it

At A Minimum. . .

- Limit access to the controlled area
- Lock the area, room or storage when unattended
- Position devices to prevent unauthorized access/viewing of information
- Follow encryption requirements

Misuse

Under Utah Code 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 the division for a purpose prohibited or not permitted by statute, rule, regulation, or policy of a governmental entity.

Reporting Misuse

For suspected misuse contact the following individuals to report:

The Commissioner of Public Safety

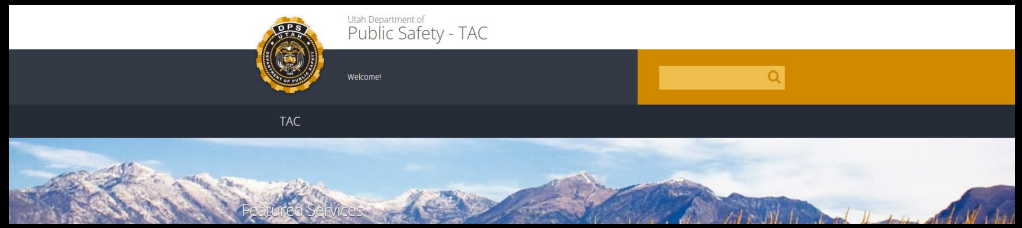
Commissioner Jess Anderson jessanderson@utah.gov
Margo Dalton modalton@utah.gov

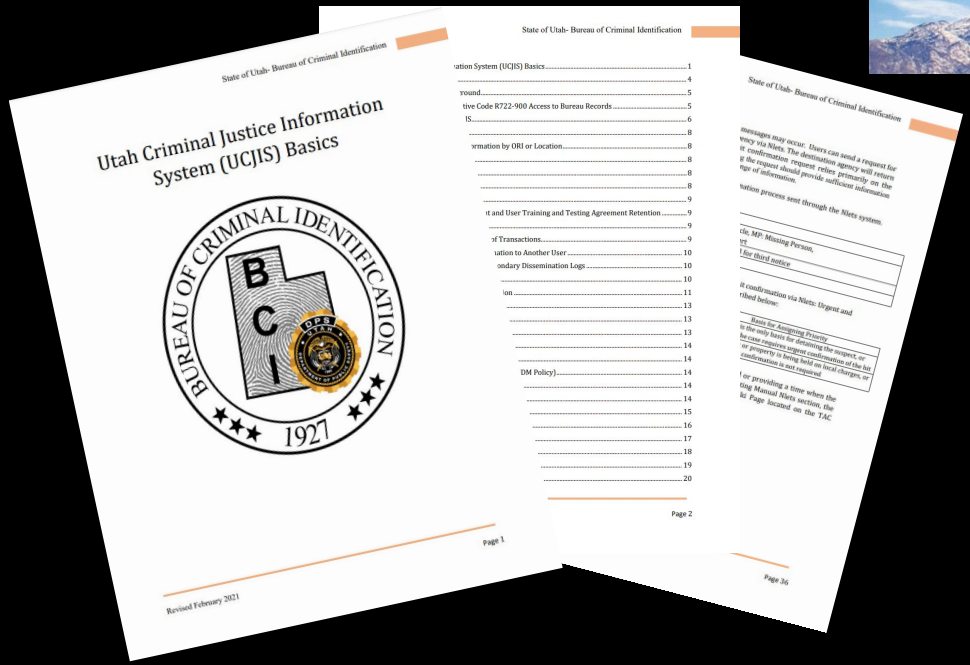
The Director of BCI

Captain Greg WIllmore gwillmor@utah.gov

Available Resources

UCJIS Basics Manual





UCJIS Basics Manual

- User Dissemination Log of Transactions
- User Disseminating Information to Another User
- Recipient Agencies and Secondary Dissemination Logs
- Motion of Discover

UCJIS Basics Manual

- Radio Frequency Dissemination
- Information Security
- Media Destruction

Presentations

2021 Virtual Regional Training

Life Cycle of a Case

Dissemination

UCJIS Updates

Felony Warrant FAQs

What's in a Protective Order? POs and JRAs

AMBER Alert Updates

Use of Force updated May 2021

Field Service Representatives

Central: gmcneil@utah.gov

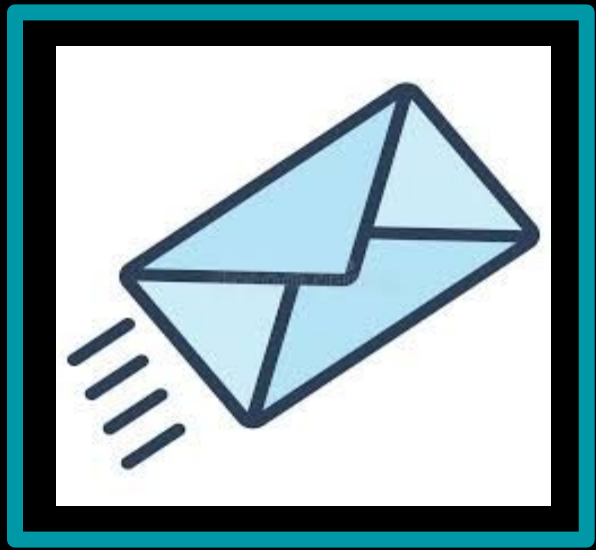
Northern: ovaisima@utah.gov

Salt Lake 1: wthomsen@utah.gov

Salt Lake 2 & UHP: jharr@utah.gov

Southern: alisalarson@utah.gov

Wasatch & Navajo Nations: chauntaybaker@utah.gov



Scenarios

Scenario 1

The friend of the son of a deputy in your agency is pulled over. His background check reveals a history of violence, fraud, an NCIC known or suspected terrorist hit and several outstanding warrants. The deputy wants to know if anything came up on his check. Can he have this information?

Scenario 1 Answer

Dissemination of this information, even within the department, is not authorized in this situation. Unless there is a valid criminal justice purpose for the dissemination, what was found through UCJIS may not be passed to the deputy.

Scenario 2

You have new renters for your basement apartment and want to screen them to ensure that you they don’t have any outstanding warrants.

Scenario 2 Answer

This type of check is not authorized through UCJIS, however on the DPS public website, there is a link to check for warrants • https://bci.utah.gov/check-your-utah-warrants/

Scenario 3

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 considered dissemination?

Scenario 3 Answer

This is considered dissemination and also misuse.Although the individual may have had good intentions – it is still not allowed.

UCJIS information is protected and should not be shared with the public

Scenario 4

A city or county legislature or representative’s aide wants to know who has parked in their parking spot or who has parked in the lot of the building. What information can you run and give to them?

Scenario 4 Answer

You cannot give them any information. They are not authorized to receive it.

Scenario 5

If an officer is driving down the road and runs the license plate of the car driving in the other lane, can the officer then run the DL of the registered owner?

Scenario 5 Answer

You can as long as it is in your agencies policy and it is for a criminal justice purpose

Scenario 6

An Attorney’s office asks the Police Department for criminal history information on an individual, can they provide that to them?

Scenario 6 Answer

If the Attorney's office has their own ORI the PD can disseminate that information to them however, If they have their own ORI should be able run the information themselves.

In the case that they do not have ORI that information can not be disseminated and they will need to apply for an ORI by emailing Whitney WIlson at wthomsen@utah.gov

Scenario 7

A user calls dispatch to run the MMJL transaction, what should they do to disseminate their findings?

Scenario 7 Answer

The Dispatcher should verify the person is a Law Enforcement User, then run it. Some agencies don’t have access.

Questions