

Utah Criminal Justice Information System (UCJIS) Basics



Utah Criminal Justice Information System (UCJIS) Basics.....	1
Introduction	4
1.0 History and Background.....	5
1.1 Utah Administrative Code R722-900 Access to Bureau Records	5
1.2 The House of UCJIS.....	6
2.0 Agency ORI	8
2.1 Finding Agency Information by ORI or Location.....	8
3.0 User and Non-User.....	8
3.1 User.....	8
3.2 Non-Access User.....	8
3.4 Non-User	9
3.5 User Security Agreement and User Training and Testing Agreement Retention	9
4.0 Dissemination	9
4.1 UCJIS Dissemination Log of Transactions.....	9
4.2 User Disseminating Information to Another User	10
4.3 Recipient Agencies and Secondary Dissemination Logs	10
4.4 Motion of Discovery.....	10
4.5 Radio Frequency Dissemination	11
6.3 Information Security	13
6.4 Media Destruction.....	13
7.0 Misuse of UCJIS Information	13
8.0 Internet Access to UCJIS.....	14
8.1 Browsers – Google Chrome	14
8.2 Laptop, Phone, & Tablet Access (MDM Policy).....	14
8.3 Network Firewall.....	14
8.4 Access through Vendors	14
8.5 Reasons for Accessing UCJIS	15
Using UCJIS	16
9.0 Login Procedures.....	17
9.1 User Authentication.....	18
10.0 UCJIS Home Page.....	19
10.1 Message of the Day (MOTDL)	20

10.2	Using the Tree or Transaction Code Box	21
10.3	Configuration: Managing Favorites and Preferences	21
10.3.1	Favorites.....	22
10.3.2	Preferences (PREFL).....	24
10.3.3	New Broadcast Message Button.....	25
10.3.4	Message Alert Button.....	25
10.3.5	Screen Size Compatibility	26
10.4	Change Password (CPWL).....	27
10.5	Entering Images to UCJIS records by EIM or QSW.....	28
10.6	Pop up Blocker stopping results in UCJIS	29
11.0	Accessing the Files of UCJIS	30
12.0	Tips and Tricks of UCJIS	30
13.0	NCIC Records.....	32
14.0	Nlets.....	33
15.0	Statewide Warrants	33
	UCJIS Messages	34
16.0	BCL Transaction.....	35
17.0	AM vs. BC Messages and YQ vs. YR Transaction Codes.....	35

Introduction



1.0 History and Background

The federal Criminal Justice Information Services (CJIS) was established in 1992 to serve as the central repository of criminal justice information services in the FBI. It is the home to an array of services that are a lifeline to law enforcement and the cornerstone of protecting the nation. The FBI has granted access to the CJIS files to BCI with the requirement of complying with all laws and regulations that surround the use of CJIS information.

The Utah Criminal Justice Information System (UCJIS) was created to house all of the federal and Utah criminal justice files. All state and federal files that are housed and accessed directly or indirectly through UCJIS are protected by state and federal laws. All of the information that is acquired through UCJIS, either printed or seen on a monitor, or communicated verbally, is confidential and is protected by Utah Code Annotated 53-10-108. Any misuse of this information could result in civil or criminal charges.

1.1 Utah Administrative Code R722-900 Access to Bureau Records

The purpose of this rule is to establish procedures whereby criminal justice agencies, qualified entities, and individuals may obtain access to the Utah Bureau of Criminal Identification within the Department of Public Safety criminal history system known as the Utah Criminal Justice Information System.

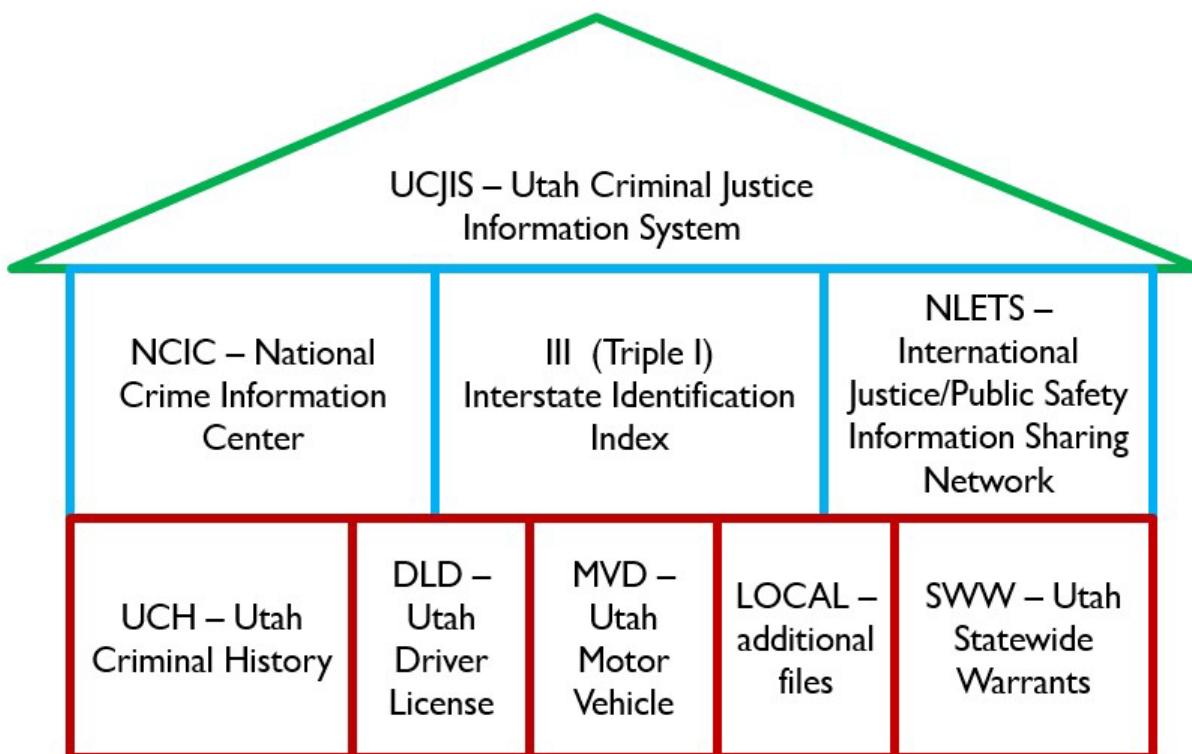
Because of the privacy and security of information acquired through UCJIS, this rule defines "criminal justice agency", the process for an agency to be given access to UCJIS, the Right of Access to this information, and the BCI audit requirements.

This rule also defines misuse as the access, use, disclosure, or dissemination of records for a purpose prohibited or not permitted by statute, rule, regulation, or policy of a government entity. The Bureau may suspend or revoke access to records by an agency, entity, TAC, user, non-user, or employee of the entity if the agency, entity, TAC, user, non-user, or employee of the entity fails to comply with any terms of signed Agency Agreement or signed User/Non-User Agreement.

To read the entire Administrative Rule governing UCJIS, see the following:
<https://rules.utah.gov/publicat/code/r722/r722-900.htm>

1.2 The House of UCJIS

The House of UCJIS is available to any authorized criminal justice agency in the state of Utah.



The House of UCJIS

The **NCIC** files contain nationwide information such as:

- Wanted persons, gangs, terrorists, missing persons, sex offenders, unidentified persons □
Stolen property, vehicles, guns, securities, identity theft

The **Triple I (III)** file provides a means of conducting national criminal history record checks. Each criminal history record is supported by a ten-print fingerprint submission.

The **Nlets** files contain information such as:

- Out-of-state criminal histories, driver license, motor vehicle registrations and Canadian files
- Homeland Security, Interpol Wanted, Immigration inquiries
- AMBER Alert, hit confirmations, administrative messages

The **Utah Criminal History (UCH)** are the criminal history records supported by fingerprints in the state of Utah. Information is supplied by the Utah criminal justice agencies to BCI, who then create, update, and maintain the records.

The **Driver License Division (DLD)** files are accessed through UCJIS and are owned and maintained by the Utah Driver License Division. The **Driver's Privacy Protection Act of 1994** is a United States federal statute governing the privacy and disclosure of personal information gathered by the Motor Vehicle Division (MVD). Disseminating driver license or motor vehicle information for non-criminal justice purposes is a violation of that federal act. These files are made available to law enforcement for criminal justice purposes. Each user accessing these files agrees to:

- Abide by all present laws, rules, policies, and procedures of the Driver License Division and Department of Motor Vehicles.
- Abide by the Federal Driver Privacy Protection Act.
- Give the information accessed only to criminal justice agencies for criminal justice purposes.
- Refer requests by private citizens for Driver License or Motor Vehicle information to the respective division to be handled in accordance with Driver License and Motor Vehicle Division policies.

The **Motor Vehicle Division (MVD)** files are accessed through UCJIS and are owned and maintained by the Utah State Tax Commission. The Driver's Privacy Protection Act of 1994 is a United States federal statute governing the privacy and disclosure of personal information gathered by Motor Vehicle Division (MVD). Disseminating driver license or motor vehicle information for non-criminal justice purposes is a violation of that federal act. Driver License and Motor Vehicle information does not fall under the management control of BCI. Please review 5.4.1 Driver License Division (DLD) for more information.

Statewide Warrants (SWW) are created by Utah Courts and maintained by criminal justice agencies. The Courts are responsible to recall, reactivate (re-issue), validate and modify a statewide warrant.

The **Department of Corrections (DOC)** allows UCJIS access to O-Track, which is created and maintained by the DOC for offenders that are under the supervision of the DOC.

Other Utah files available in UCJIS include, but are not limited to the following:

- Crash & Citation
- Court Case Inquiry
- Crime Lab
- Jail Release Agreements
- eWarrants
- Probable Cause Affidavits

2.0 Agency ORI

The federal NCIC ORI (Originating Agency Identifier) is a nine-character identifier assigned by the FBI to an agency that has met the established qualifying criteria. Utah agency ORIs begin with UT followed by their county code i.e. UT003 is the beginning of all agencies in Cache County. Criteria for the assignment of an ORI is used to determine whether or not a law enforcement agency qualifies for use of the NCIC. The agency ORI should not be confused with the agency ID. The agency ID is between four and six alpha characters only and is an abbreviation of the agency name assigned by BCI i.e. the agency ID for Moab Police Department is MOABPD. For additional information, review the ORI section of the NCIC Operating Manual located on the TAC Website.

2.1 Finding Agency Information by ORI or Location

UCJIS users can use NCIC to obtain information about an agency when only that agency's ORI is known. To check NCIC from the UCJIS Home page, enter **Q0** (Q-zero) into the "Transaction Code" box and hit enter. Or from the UCJIS Tree, click "Other", then "NCIC", then "ORI Maint", then "Q0 Translate ORI #". More information can be found in the NCIC Operating Manual.

The Nlets ORION file allows an operator to determine the ORI of a Nlets user when only the location (city and state) or federal agency name and state are known. This file also gives users the capability to inquire upon any ORI and receive the agency name, address, and telephone number in the response. This information aids in hit confirmations. To use the Nlets system from the UCJIS Home page, enter **TQ** into the "Transaction Code" box and hit enter. Or from the UCJIS Tree, click on "Other", then "Nlets", then "ORI Maint", then "TQ Query ORI". For additional information, review the Nlets User Policy Manual located on the TAC Website.

3.0 User and Non-User

There are two different types of 'users' and one type of 'non-user'. All users and non-users need to be fingerprinted, have a signed User/Non-user Security Agreement submitted to BCI and enrolled in Rap Back before they can access or be around UCJIS information, or have unescorted access into an agency. All users will have their own password. They will also have their own unique personal ID number to identify themselves when calling into the UCJIS Help Desk. The password and personal ID should never be shared with anyone.

3.1 User

A user is a person working for or with an agency who has direct access to UCJIS. A user must be fingerprinted, enrolled in Rap Back, and have signed a User Security Agreement prior to accessing any file in UCJIS. All users are trained and tested initially and every two years thereafter. All users must sign the User Training and Testing Agreement every two years after testing.

3.2 Non-Access User

A non-access user is a person in the criminal justice industry who can request and receive UCJIS information from a user who has access to UCJIS. A non-access user must be fingerprinted, enrolled

in Rap Back, and have signed a User Security Agreement prior to receiving any information from UCJIS. All non-access users are trained initially and every two years thereafter. All non-access users must sign the User Training and Testing Agreement every two years after training.

3.4 Non-User

A non-user is anyone that has unescorted access to the computer terminal areas where information may be available either on a monitor, printer, or by verbal exchange. A non-user includes IT (LASO Local Agency Security Officer) which is an agency's information technology specialist. A non-user must be fingerprinted, enrolled in Rap Back, and have signed a Non-User Security Agreement prior to being given unescorted access. All non-users are trained initially and every two years thereafter.

3.5 User Security Agreement and User Training and Testing Agreement Retention

User/Non-user Security Agreements are a one-time document. This agreement should be retained for the duration of the employment of the user/nonuser up until the end of the audit cycle (three years) in which they left the employment of the agency or was terminated. For example, if the audit cycle is 2017-2020 and the user left the agency in 2019, the agency would keep the agreement filed until July 2020. Once the audit cycle has ended, the agency can cross-cut shred/burn the document.

User Training and Testing Agreements are signed and submitted to BCI every two years. You must retain the most recent copy for the duration of the audit cycle (three years). If an agency has a user that leaves their employment or is terminated, they must retain the document until the end of the audit cycle in which the user left or was terminated. Once the audit cycle has ended, the agency can cross-cut shred/burn the document.

4.0 Dissemination

Dissemination is the act of spreading or circulating information. 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 Annotated 53-10-108. The act of 'dissemination' with regards to UCJIS information is most commonly associated with the following: UCJIS dissemination (UCJIS keeps a log of the transaction); a user disseminating information to another user; and a user disseminating information to recipient agencies.

4.1 UCJIS Dissemination Log of Transactions

Each time a user requests or 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 following on each request:

- Date and time
- User ID of the person and agency making the request
- File accessed
- Search criteria

4.2 User Disseminating Information to Another User

In many agencies, there are users or non-access users who are authorized to request UCJIS information from other users. One example is a patrol officer who calls into dispatch to 'run a plate'. The dispatcher tells the patrol officer what was discovered about the plate – that is one user disseminating information to another user. When a user or non-access user requests information from another user, it is not necessary to keep a separate log of this transaction. UCJIS is maintaining the dissemination log of transactions.

4.3 Recipient Agencies and Secondary Dissemination Logs

There are criminal justice agencies that have not acquired an ORI from the FBI, but still receive UCJIS information from an agency with an ORI. If an agency provides any information from UCJIS to another criminal justice agency or for Motion of Discovery purposes, it is considered secondary dissemination. 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. The administrators of both agencies must sign the UCJIS Information Exchange Agreement.

When a servicing agency releases information from UCJIS to another agency, a Secondary Dissemination log must be maintained at the servicing agency. 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. The recipient agency must be trained by the servicing agency on dissemination, privacy, and security of UCJIS information.

An authorized agency servicing another authorized agency must assume responsibility for and enforce system security with regard to the agency that is serviced.

4.4 Motion of Discovery

In court proceedings, defense attorneys are allowed the dissemination of criminal history records, a Utah criminal history, and/or III criminal history under "Motion of Discovery". Information from any other file in UCJIS is prohibited unless court-ordered. Prosecutors are required by law to provide only information they have obtained for their case. If defense attorneys request any additional UCJIS information, they must obtain a court order signed by the judge and present it to BCI.

BCI requires that agencies disclosing UCJIS information in this manner maintain a Secondary Dissemination Log that includes the date of dissemination, the person requesting the record, and the intended purpose. BCI also suggests a UCJIS Information Exchange Agreement be in place between the entities.

Each page of criminal history should contain a statement reminding the receiver of the document that further dissemination to any unauthorized person or agency may result in both civil and criminal penalties. For further information, refer to the UCH section of the BCI Operating Manual.

4.5 Radio Frequency Dissemination

The Utah Department of Public Safety (DPS) and BCI do not have policies that impose restrictions on the dissemination of UCJIS information over law enforcement radio frequencies. This applies to authorized and legislated law enforcement agencies in Utah as defined in Section (53-13) of the Utah Code Annotated. State, county, and local law enforcement agencies are encouraged to develop policy guidelines as to when and under what circumstances criminal history information (both Utah and Triple I) may be disseminated over their respective radio channel(s). Agencies also need to be familiar with the Triple I policy concerning radio transmission of criminal history information.

When developing local dissemination policies, agencies need to recognize that criminal history information is sensitive in nature. Because many different agencies are involved in developing an individual's criminal history, the information can be incomplete and at times inaccurate. Particular attention should be given to the fact that many members of the public use police scanners, and dissemination of criminal justice information.

5.0 Privacy

The definition of privacy is the state or condition of being free from observation or disturbance by others. Any information acquired from any file in the house of UCJIS is for criminal justice purposes only. Computer monitors, laptops, and tablets must not be in the view of the public. When hard copies of UCJIS information are no longer needed, they must be destroyed by either shredding or burning.

6.0 Security

The definition of security is the state of being protected. BCI suggests that each agency have guidelines for protecting UCJIS from unauthorized persons. Misuse of information received directly or indirectly from UCJIS can result in civil or criminal penalties per UCA 53-10-108.

6.1 User Security

All new users accessing UCJIS must undergo an FBI fingerprint-based background check per CJIS Policy. The UCJIS name-based background check is optional as of September 2018. If your agency chooses to run a name-based background check, it must be run prior to creating their login ID. Each UCJIS user must have their own login ID. Users must never share logins, even for training purposes.

6.2 Workplace Security

Be aware of your computer monitor and what can be viewed on the monitor from your office doorway or window. Monitors should not be located where a passerby could see what is on the screen. A computer must never be left unlocked when the user is away. The computer site and/or terminal area must have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment or to any of the case files where UCJIS information is stored. Officers who access the UCJIS files in their vehicles must ensure that the monitor cannot be seen by the public. All mobile devices (laptops, tablets, phones) that access UCJIS must be registered with DPS DTS as of July 1, 2015.

Anyone who has unescorted access (a non-user) to terminal areas where the files containing UCJIS information are located must have undergone a name and fingerprint-based background check. All visitors to computer centers and/or terminal areas must be accompanied by an authorized person at all times. A visitor is anyone who has not undergone a name and fingerprint-based background check.

6.3 Information Security

All printed information acquired through UCJIS including the BCI, NCIC, and Nlets manuals are confidential. All documentation that is no longer needed must be physically destroyed by either shredding or burning. If the agency has a contract with a vendor that picks up locked shred containers to take UCJIS information off-site for destruction, either a UCJIS user must go to the destruction site to witness that the information is destroyed, or the entire shredding company must be set up with the agency as non-users. This would address the need for 'authorized persons' witnessing the destruction of UCJIS information.

6.4 Media Destruction

Any CDs/Diskettes/Thumb drives must be destroyed when no longer used. All computer hard drives must be wiped (per the Department of Defense 522022M Disk Wipe Standards) or physically destroyed.

7.0 Misuse of UCJIS Information

All of the information acquired from any file accessed in UCJIS is governed by the dissemination, privacy, and security regulations and policies of the FBI and the state of Utah. UCJIS information is for criminal justice investigations and criminal justice employment only.

Misuse of UCJIS information: Violation of dissemination, privacy, and security regulations can result in criminal prosecution of the person(s) involved and loss of state computer access by the agency. There is also the potential for civil sanctions as well. BCI maintains an automated dissemination log of all UCJIS transactions to help ensure that this information is being accessed for proper reasons. Dissemination of criminal history record information is controlled by federal regulations and Utah State Law. 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 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.

Inquiring into any of the UCJIS files is NOT permitted for the following purposes: curiosity and personal inquiries, employment for non-criminal justice purposes, business licenses, military recruiters, city/county employees, citizen advisory boards, etc.

When a person discovers or becomes aware of any unauthorized use of records created or maintained by BCI, the agency administrator or the agency TAC must inform the DPS Commissioner and the Director of BCI as per Utah Code Annotated 53-10-108. Please also notify the BCI Field Services Supervisor at 801-281-5098.

8.0 Internet Access to UCJIS

UCJIS is a web-based system that is being accessed from many different devices. This includes mobile devices such as smart phones, tablets, laptops, etc. No matter which device is used, dissemination, privacy, and security laws governing misuse of UCJIS information all apply. Agencies accessing UCJIS through an Internet Service Provider (ISP) are required to have firewalls in place.

8.1 Browsers – Google Chrome

UCJIS can be accessed through Mozilla Firefox and Google Chrome. In any browser that is used, it is important to clear the cache and browser history on a regular basis (suggested at least weekly) so that UCJIS will run and display information accurately and confirm that POP UPS are allowed. There are several transactions in UCJIS that work better with a specific browser. When printing a Utah criminal history, please use Google Chrome. When accessing the TAC Website, it is better to access this site using Google Chrome. UCJIS will not work efficiently in Internet Explorer.

8.2 Laptop, Phone, & Tablet Access (MDM Policy)

Any portable device that is used to access UCJIS is under the same dissemination, privacy, security and misuse regulations as a desktop computer located in a locked office. All mobile devices are restricted under Mobile Device Management (MDM) and must be registered with the state if used to access the secured state wireless network. If you have any questions, please contact the DTS Help Desk at 801-965-4066. There is also a self-help web portal on the DTS website at dts.utah.gov under Get Help/Other/MDM Help.

Agencies using mobile devices must have an MDM policy in place before BCI can grant access to UCJIS. The policy would include the name of the MDM vendor. All MDM vendors must meet CJIS Security Policy requirements.

8.3 Network Firewall

Agencies must have a firewall in place if they access the UCJIS system through the state WAN (Wide-Area Network). Agencies that access UCJIS using another method, such as an Internet Service Provider (ISP) or have an ISP connection in addition to the WAN connection are required to have firewalls in place. Additional information regarding these firewalls may be obtained from Utah's DTS department.

8.4 Access through Vendors

Many agencies use vendors such as Spillman, Fatpot, Versaterm, eForce, etc. to access UCJIS. Whether the information comes directly from UCJIS or through a vendor, it is all protected by state and federal regulations. The password that is used to access the vendor program cannot be the same as the UCJIS password. There may be times when a user is locked out of the vendor program. The UCJIS Help Desk cannot assist with vendor issues.

8.5 Reasons for Accessing UCJIS

UCJIS can only be used for criminal justice purposes. This is defined as the “administration of criminal justice” or “criminal justice employment.” The term “administration of criminal justice” is defined by the FBI as the performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, and rehabilitation of accused persons or criminal offenders.

Using UCJIS



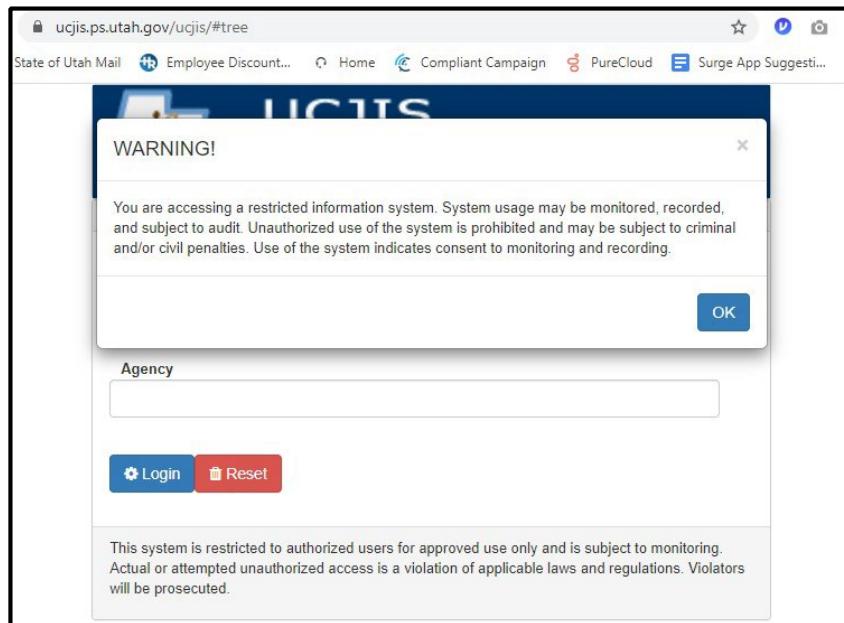
9.0 Login Procedures

Prior to accessing UCJIS, the agency TAC (Terminal Agency Coordinator) will have given the user their user ID, the agency ID, and a temporary password. These are each case sensitive.

Please read the WARNING! This warning will appear each time a user logs into UCJIS. Acknowledge the warning by clicking OK. Enter your individual user ID and your agency ID.

Throughout UCJIS, the TAB key or mouse will move the cursor from one field to another. When you hit ENTER, it performs the same function as SUBMIT.

UCJIS LOGIN



The icon next to SUBMIT will spin when the system is processing your request.

9.1 User Authentication

The User Authentication fields will appear the first time a user enters UCJIS. This registration will connect a specific user ID with their specific IP address. Begin by entering the user's temporary password which is provided by the TAC after access to UCJIS has been granted by the UCJIS Help Desk. Click on SUBMIT.

USER AUTHENTICATION

REGISTRATION REQUIRED

The registration process involves two steps:

1. Selecting one of many available images and entering a passphrase that will be presented to you each time you authenticate to the UCJIS system.
2. Selecting between an email address and cell phone to provide a PIN.

Password

Submit

This system is restricted to authorized users for approved use only and is subject to monitoring. Actual or attempted unauthorized access is a violation of applicable laws and regulations. Violators will be prosecuted.

Select an image, create a pass phrase and select a method of verification.

Select an image.

NOTE: This image will be displayed at each login to ensure that you are logging in to the authentic UCJIS site.

Click here to retrieve images for selection

Please create a pass phrase.

NOTE: Your pass phrase is NOT your password. It is a message that you will know you have entered yourself. It will be shown at each login and should not contain any passwords or confidential information.

Pass phrase:

Select a method of verification.

E-mail Text Message Google Authenticator

Submit

Select an image and create a pass phrase that the user will recognize while logging into UCJIS. Then select the method of verification: email, text message, or Google Authenticator. The user will receive a PIN number that is required to access UCJIS. The PIN number must be entered within five minutes or it will expire.

A verification email would look like this:

□ ☆ □ UCJIS

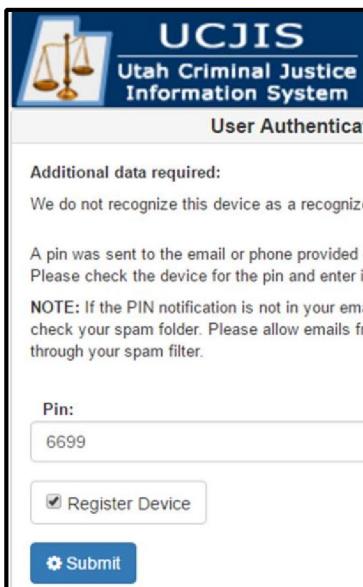
UCJIS Email Verification - Verification Code: 6699 Enter verification code in UCJIS to verify your email address.

A verification text would look like this:

Subject:UCJIS
Identification
Code
Identification
Code: 32261

Enter online at
prompt. Code
is only valid for
5 minutes

Enter the PIN number and SUBMIT. This specific device and specific user ID have been registered.



The form is titled "UCJIS Utah Criminal Justice Information System User Authentication". It includes a logo of a scale of justice. The "Additional data required" section states: "We do not recognize this device as a recognized device. A pin was sent to the email or phone provided. Please check the device for the pin and enter it." A note says: "NOTE: If the PIN notification is not in your email, check your spam folder. Please allow emails from UCJIS through your spam filter." The "Pin:" field contains "6699". There is a checked checkbox for "Register Device" and a blue "Submit" button.

After clicking on SUBMIT, a window will appear offering congratulations for completing the UCJIS Advanced Authentication registration.

Click OK to login to UCJIS through the new authentication process.

The UCJIS login screen will appear.

Login with the user ID and agency code.

The next screen to appear should have the image and pass phrase selected by the user. If for any reason these items do not appear, or they are different from what the user selected, contact the UCJIS Help Desk at 801-965-4446.

10.0 UCJIS Home Page

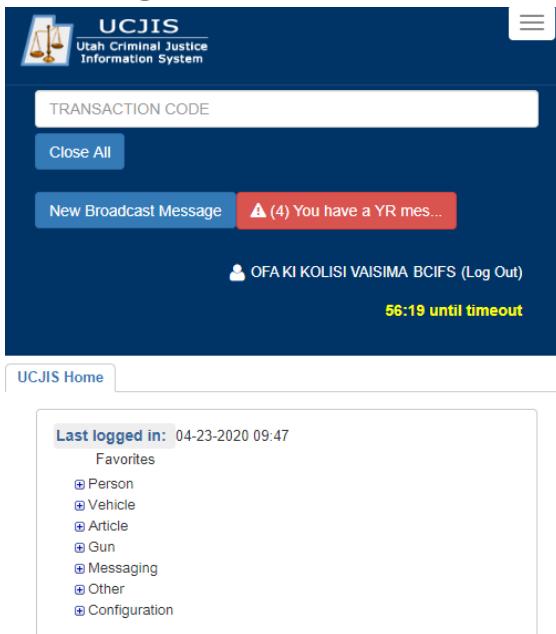
From the UCJIS Home page, a user can access any file that their agency has access to by using the TREE or the "Transaction Code" box. The Home Page contains the "Message of the Day" from BCI for statewide information regarding UCJIS updates, upcoming trainings, system changes, or down time. The Home Page also reminds the user when their password is going to expire if the expiration is within fourteen days. In the upper right-hand corner under "Username" and "Logout" is the session 'timeout' clock. To reset the clock, click on the UCJIS Home tab or submit a new inquiry/entry into UCJIS.

10.1 Message of the Day (MOTDL)

The Message of the Day (MOTD) window is displayed in front of the home page for easier reading. To access a previous MOTD from the tree, MOTD is located under Messaging/Local/MOTD, or type in MOTDL in the transaction code box.

The screenshot shows a web-based application window titled "UCJIS Home MOTDL". The main title bar has "UCJIS Home" and "MOTDL" with a close button. Below the title bar is a "Query" button. The main content area has a blue header bar with the text "Message of the Day". The first section is titled "Search Parameters" and contains fields for "Search Text" (a text input box), "Icon Type" (a dropdown menu with options: VALIDATIONS, CAUTION, INFORMATION, and URGENT, where "VALIDATIONS" is highlighted), and a "View Active" button. The second section is titled "Time Frame Parameters" and contains fields for "Timeframe" (a dropdown menu), and "Start Date Time" and "End Date Time" (each a group of three input boxes for MM, DD, and YYYY). The "Start Date Time" group has dropdown menus for the month and year, and an input box for the day. The "End Date Time" group has dropdown menus for the month and year, and an input box for the day.

10.2 Using the Tree or Transaction Code Box



The screenshot shows the UCJIS Home page. At the top, there is a 'TRANSACTION CODE' input field and a 'Close All' button. Below that, a message says 'New Broadcast Message' and '⚠ (4) You have a YR mes...'. The top right shows a user icon and 'OFA KI KOLISI VAISIMA BCIFS (Log Out)'. A yellow timer at the top right says '56:19 until timeout'. At the bottom left is a 'UCJIS Home' button. The main content area is a box titled 'Last logged in: 04-23-2020 09:47'. It contains a 'Favorites' section with a plus sign icon and a list of categories: Person, Vehicle, Article, Gun, Messaging, Other, and Configuration.

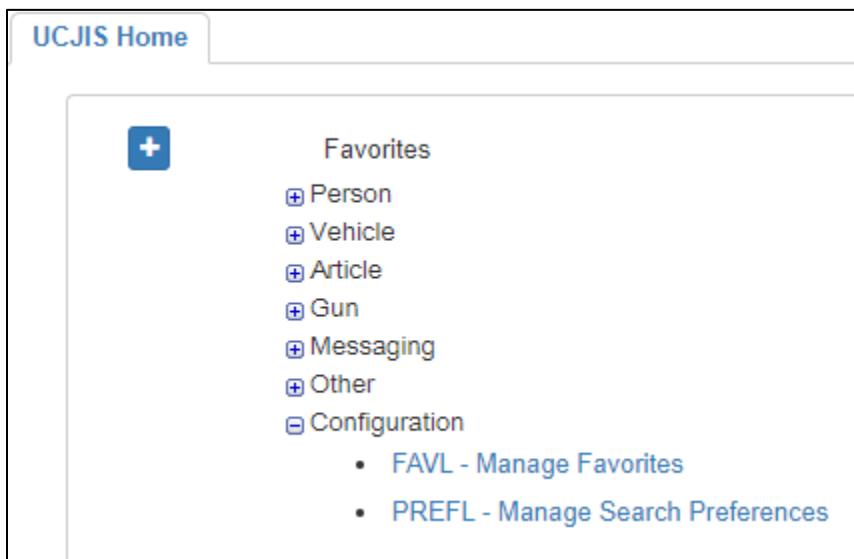
The list of categories on the left side of the Home Page is called the TREE. Click on the **+** to expand the TREE and all files available to the user will be displayed. To collapse the TREE, click on the **-**.

To open a specific category, click on the plus sign **+** next to the name, and the files that are available will appear. To close a category, click on the minus sign.

All transactions in UCJIS can be accessed by either clicking on the file from the TREE or by entering the transaction code into TRANSACTION CODE box.

10.3 Configuration: Managing Favorites and Preferences

To set up specific FAVORITES and PREFERENCES, select CONFIGURATION.



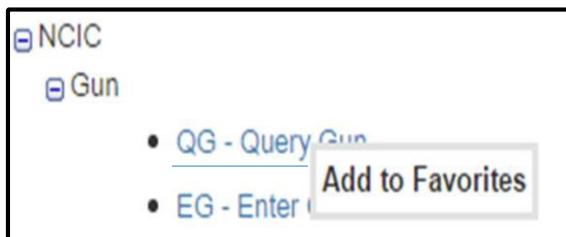
The screenshot shows the UCJIS Configuration page. At the top left is a 'UCJIS Home' button. The main content area has a plus sign icon and a 'Favorites' section. It lists categories: Person, Vehicle, Article, Gun, Messaging, Other, and Configuration. Under Configuration, there are two items: 'FAVL - Manage Favorites' and 'PREFL - Manage Search Preferences'.

10.3.1 Favorites

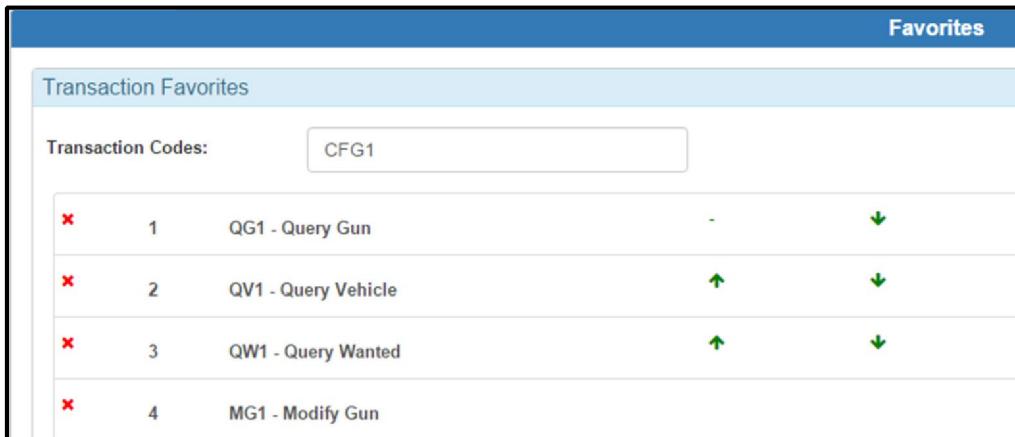
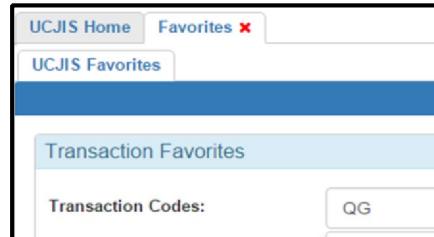
“Favorites” allows the user to set up a list of their most-used transactions. There are two ways to create a list of Favorites: using the right click of the mouse from the tree or by entering the transaction code into the Favorites transaction code box.

From the Tree, open to the specific transaction code while hovering over the transaction, and the transaction becomes underlined. With the transaction underlined, right-click on the mouse and “Add to Favorites”.

Underlined and using the right-click:



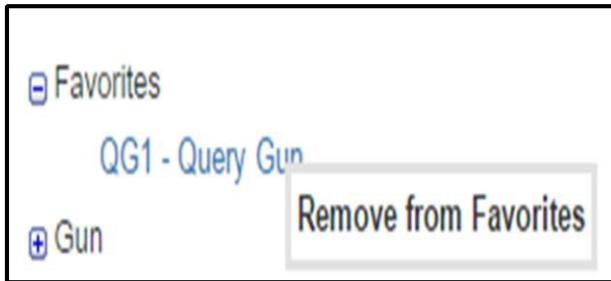
Or enter the transaction code:



The specific transaction code can also be entered into the “Transaction Codes” box under the “Favorites” Tab. Either way, the transaction is added to a user’s “Favorites”.

To change a user's "Favorites", access the specific transaction code in the tree and hover over it to get the underline, then use the right-click to remove the transaction. A user can also access the Favorites transaction and click on the red X:

Remove by right-click:



Remove by red X:



To reorder the "Favorites" in the tree, drag and drop the transaction to the desired location. A user can also access the "Favorites" transaction and use the arrows to reorder:

Whenever a change is made to a user's "Favorites", a window will appear indicating the "Favorites" have been updated.



10.3.2 Preferences (PREFL)

Under “Configuration”, users have the option to manage personal default preferences, which help to streamline search criteria. In PREFERENCES, the user has the option to view UCJIS in the Default Color Scheme or in Night Mode.

The image contains two side-by-side screenshots of the UCJIS User Preferences page. Both screenshots have a header with 'UCJIS Home' and 'Preferences' buttons, and a sub-header 'UCJIS User Preferences'.

Top Screenshot (Light Theme):

- Color Scheme:** A dropdown menu set to "DEFAULT COLOR SCHEME".
- Display:**
 - Popup Alerts
 - Default Requestor
 - View NLETs Criminal History in Text

Bottom Screenshot (Dark Theme):

- Color Scheme:** A dropdown menu set to "NIGHT MODE".
- Display:**
 - Popup Alerts
 - Default Requestor
 - View NLETs Criminal History in Text

“Preferences” also gives users the option to change inquiry search criteria defaults on the following Utah files: Protective Orders, Statewide Warrants, Warrants by Zip Code, Motor Vehicle, Criminal History, and Driver License.

The name search preference has four options: Starts With, Exact, Contains, and Phonetic.

The image shows a screenshot of the UCJIS User Preferences page with two sections: "PO Query Defaults" and "SWW Query Defaults".

PO Query Defaults:

- Last Name Search Type:** A dropdown menu set to "STARTSWITH".
- DOB Search Type:** A dropdown menu set to "EXACT".
- First Name Search Type:** A dropdown menu showing options: STARTSWITH, EXACT, CONTAINS, and PHONETIC. The "STARTSWITH" option is highlighted.

SWW Query Defaults:

- Last Name Search Type:** A dropdown menu set to "STARTSWITH".
- DOB Search Type:** A dropdown menu set to "EXACT".
- First Name Search Type:** A dropdown menu set to "STARTSWITH".

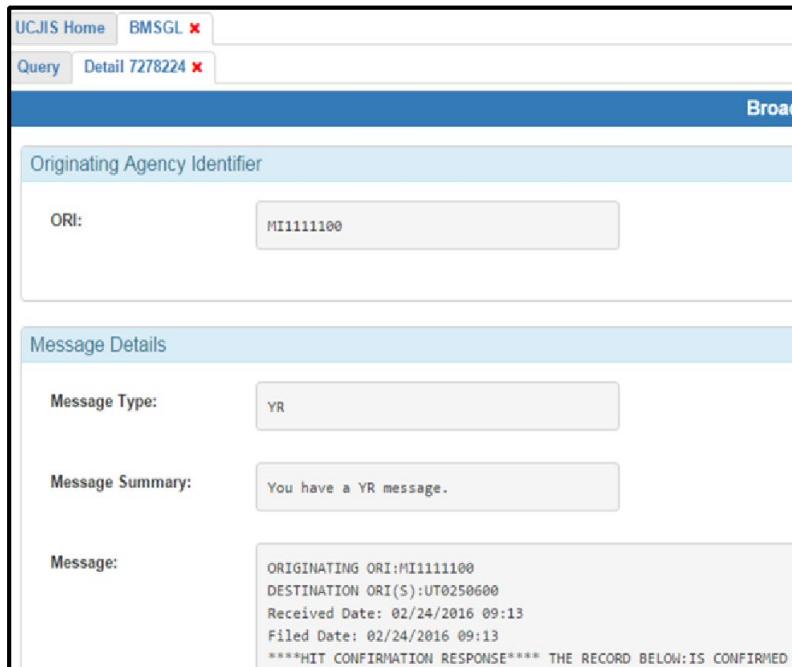
10.3.3 New Broadcast Message Button

The “New Broadcasts” button is a directory of incoming and outgoing messages which resets each day at midnight. These messages are sent from NCIC, Nlets, BCI, and other agencies. By clicking on this button, an agency is able to see messages that have not previously been read by the agency. If all messages have been viewed, this button will not be displayed. Previously read messages can be accessed through the BMSGL transaction.

The BMSGL transaction allows an agency to acquire the NCIC dollar (\$) messages such as \$F, \$P, \$H, \$K, etc. For more information about the NCIC dollar messages, see the NCIC Operating Manual Introduction and the BCI Operating Manual Nlets section. Users have the option to select default timeframe options, or to specify the start and end date time.

10.3.4 Message Alert Button

The red Message Alert button has replaced the previous scrolling alert message. These messages need the agency's attention as soon as possible. Click on the button and the message will be displayed:



The screenshot shows a web-based application interface for the UCJIS Home BMSGL transaction. At the top, there are navigation buttons: 'UCJIS Home' (disabled), 'BMSGL' (disabled), 'Query', and 'Detail 7278224'. The main content area has a blue header bar with the word 'Broad'. Below this, there are two sections: 'Originating Agency Identifier' and 'Message Details'. The 'Originating Agency Identifier' section contains an 'ORI' field with the value 'MI1111100'. The 'Message Details' section contains a 'Message Type' field with 'YR' and a 'Message Summary' field with the text 'You have a YR message.' At the bottom of the 'Message Details' section, there is a 'Message' block containing the following text:
ORIGINATING ORI:MI1111100
DESTINATION ORI(S):UT0256600
Received Date: 02/24/2016 09:13
Filed Date: 02/24/2016 09:13
****HIT CONFIRMATION RESPONSE**** THE RECORD BELOW:IS CONFIRMED

10.3.5 Screen Size Compatibility

If UCJIS is being viewed from a mobile device, all of the information is still available in its entirety and will be aligned with the left margin. Smaller screen sizes will collapse the UCJIS header. Click

the  button in the top right-hand corner of UCJIS to expand and reveal the TRANSACTION CODE box.



This screenshot shows the UCJIS interface with the transaction code box collapsed. The page title is "Utah Driver License Details [Show All] [Hide All]". The main content area displays various driver license details for subject BEAR, YOGI - 172443851. The transaction code box is visible at the bottom of the page.

License Number:	172443851
ID Number:	215915
Name:	YOGI BEAR
Date of Birth:	02/11/1950
Age:	66
License Status:	CANCELED LICENSE
Expires:	02/11/2018
TYPE:	TYPE:DUPLICATE
Class:	D
Address:	4501 S 2700 W WEST VALLEY UT 84119 COUNTY: SALT LAKE
UPDATED:	02-04-2009
SSN/TIN:	111111111
Sex:	MALE
Height:	605
Weight:	380
Eye:	BRO
Hair:	BRO

Click here to view OTRK info for subject (LEGAL STATUS PROBATION, OFN: 215915)



This screenshot shows the UCJIS interface with the transaction code box expanded. The expanded box contains the text "Click here to view OTRK info for subject (LEGAL STATUS PROBATION, OFN: 215915)" and "Capture Date: 10-12-2005". Below this is a cartoon illustration of a brown bear wearing a green cap and a white shirt. The expanded box is divided into sections: "Driving Restrictions (1)", "Alerts (1)", "THIS IS A TEST RECORD", "Miscellaneous", and "Registered Sex Offender".

Click here to view OTRK info for subject (LEGAL STATUS PROBATION, OFN: 215915)
Capture Date: 10-12-2005

Driving Restrictions (1)
1: OXYGEN WHILE DRIVING. Code: J

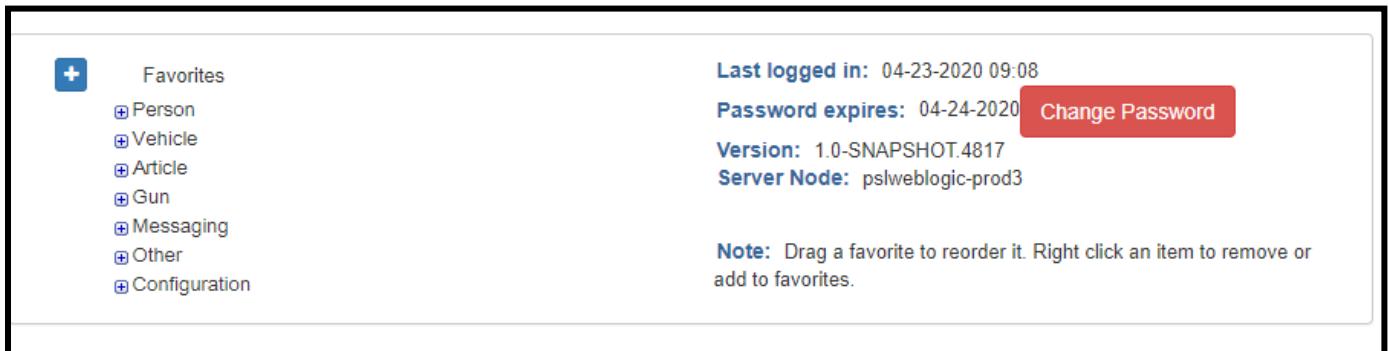
Alerts (1)
THIS IS A TEST RECORD

Miscellaneous
Concealed Firearm:
NOT FOUND
Expiration Date:
No

Registered Sex Offender:

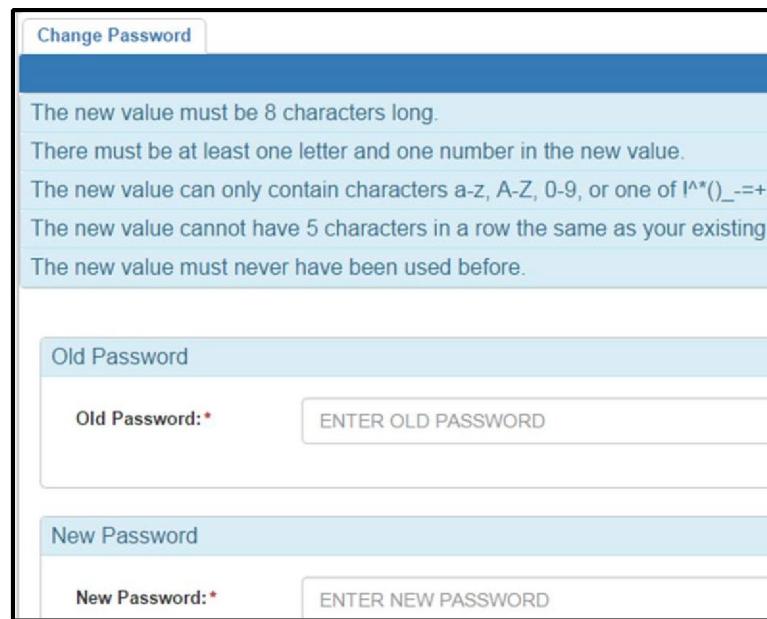
10.4 Change Password (CPWL)

The UCJIS Home Page will remind users when their password is about to expire. When the message to “Change Password” appears, the user has fourteen days to change their password.



The screenshot shows the UCJIS Home Page. On the left, there is a sidebar with a '+ Favorites' button and a list of items: Person, Vehicle, Article, Gun, Messaging, Other, and Configuration. On the right, there are several status indicators: 'Last logged in: 04-23-2020 09:08', 'Password expires: 04-24-2020', 'Version: 1.0-SNAPSHOT.4817', and 'Server Node: pslweblogic-prod3'. A red button labeled 'Change Password' is highlighted. Below these, a note says: 'Note: Drag a favorite to reorder it. Right click an item to remove or add to favorites.'

The CPW transaction informs users of the format required for the new password. Passwords must be **8 characters long**. If a user forgets his/her password, the user must contact their agency TAC to reset the password, or call the UCJIS Help Desk at 801-965-4446.



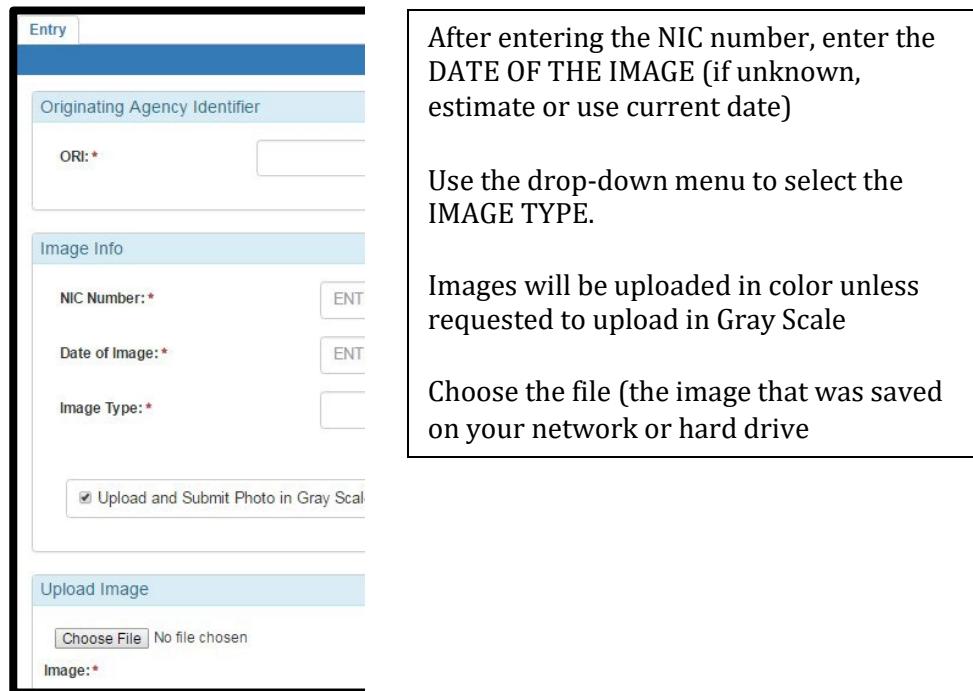
The screenshot shows the 'Change Password' transaction window. At the top, a 'Change Password' button is visible. Below it, a series of validation rules are listed in a light blue box: 'The new value must be 8 characters long.', 'There must be at least one letter and one number in the new value.', 'The new value can only contain characters a-z, A-Z, 0-9, or one of !^*()_-=+.', 'The new value cannot have 5 characters in a row the same as your existing.', and 'The new value must never have been used before.' Below these rules, there are two input fields: 'Old Password' and 'New Password'. Each field has a label on the left ('Old Password:' and 'New Password:' with a red asterisk) and a text input box on the right labeled 'ENTER OLD PASSWORD' and 'ENTER NEW PASSWORD' respectively.

10.5 Entering Images to UCJIS records by EIM or QSW

BCI encourages all agencies to add images to their records. This will aid law enforcement in the positive identification of a person or property. Images can be obtained from any source: digital camera, scanner, email, O-Track, Driver License.

After the image is acquired, save the image where it is easy to find. Save the image to the agency's network or personal computer hard drive.

Before an image can be added to a NCIC record, the image must be saved to your computer and the entry must have a NIC number. The Enter Image (EIM) transaction is used or from the UCJIS Tree, the transaction is Person, Entry, NCIC, Enter Image:



Entry

Originating Agency Identifier

ORI: *

Image Info

NIC Number: *

Date of Image: *

Image Type: *

Upload and Submit Photo in Gray Scale

Upload Image

Choose File No file chosen

Image: *

After entering the NIC number, enter the DATE OF THE IMAGE (if unknown, estimate or use current date)

Use the drop-down menu to select the IMAGE TYPE.

Images will be uploaded in color unless requested to upload in Gray Scale

Choose the file (the image that was saved on your network or hard drive)

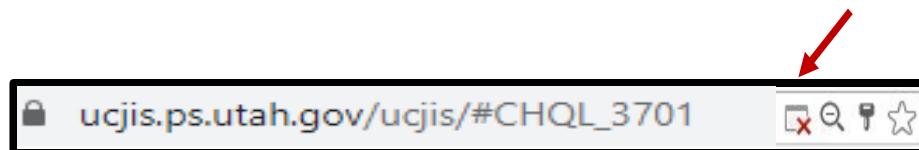
For images to be entered into Utah Statewide Warrants, query on the warrant using QSW. Add the photo using the “Add Info” button inside of the warrant and the “Add Subject Photo” window will appear:

Add Subject Photo	
Photo:*	<input type="file"/> C
Photo Type:*	<input type="text"/> C
Description:*	<input type="text"/> E

Upload the photo from your network or computer
PHOTO TYPE is either from a Booking Photo or a photo of Scars, Marks, or Tattoos
Enter a description to identify the photo

10.6 Pop up Blocker stopping results in UCJIS

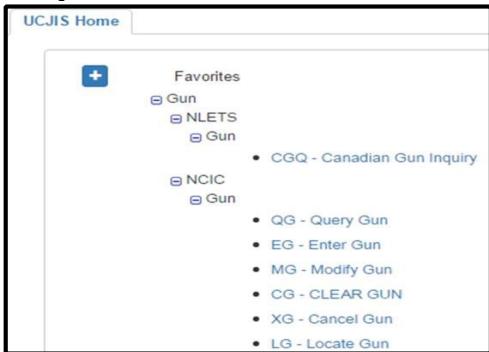
Different functions within UCJIS may require that the pop-up blockers are turned off. If a requested result fails to appear, double check the address line for the document with the red 'x' indicating that the pop up for this transaction is being blocked:



11.0 Accessing the Files of UCJIS

All files in UCJIS are categorized. Both the inquiry and entry transactions are located in the same category. By clicking on either the name of the category, or the plus sign to the left of the name in the TREE, the transactions that the user has access to will be displayed.

Example of GUN files:

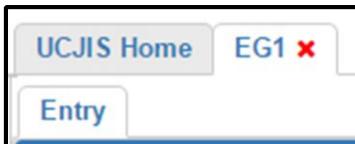


Example of MESSAGING files:

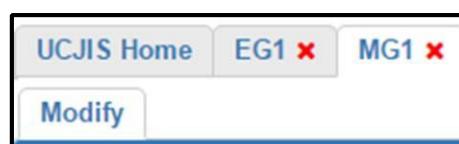


When a transaction is accessed, a tab will appear next to the UCJIS Home Tab. This system is designed to allow the user to multitask by opening different searches (organized by tabs) for a more comprehensive view of a record. For example, a gun needs to be entered into NCIC, then modified and cleared. Each transaction is organized by tabs, and the open tab is highlighted. The actual file will appear below the row of tabs under the title of the transaction (Entry, Modify, Clear).

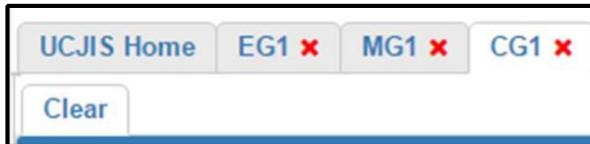
Enter NCIC gun:



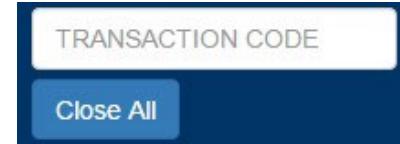
Modify NCIC gun:



The Clear transaction:



Close all tabs:



The user can go back and forth between the tabs without losing any of the information that was acquired. When the inquiry or entry is complete, use the “x” to close each individual tab or the “Close All” button located in the header under the “Transaction Code” Box.

UCJIS files can also be accessed by entering the file transaction code into the “Transaction Code” box. This text box populates a predictive drop-down list of all accessible transactions that begin with the first given letter. For example, entering MI into the transaction box will predict the following transactions based this user’s permissions:

If Multiple Transaction Inquiry is the desired transaction, be sure to enter MIL into the transaction code field. If you just accept the first code that appears, you might not receive the desired transaction.

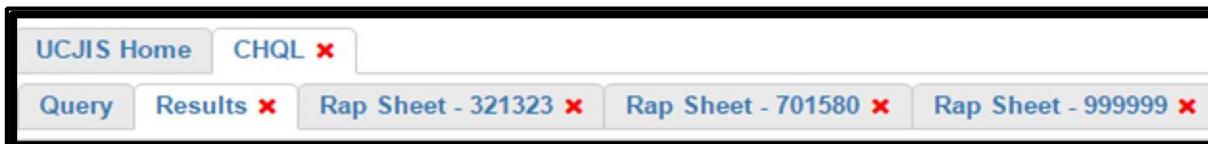


11.1 Utah Criminal History (CHQL)

When inquiring on a person in CHQL the exact name might not know, so only part of the name is entered. UCJIS will search all matches of the partial name and display all names in a ‘Query Results’ list:

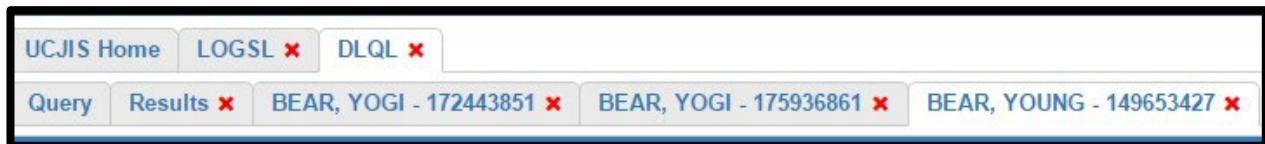
Last Name	First Name	Middle	DOB	AKA	SID #
BEAR	YOGI		02-11-1950		321323
BEAR	YOGI		02-11-1950	*	321323
BEAR	YOGI		02-11-1950		701580
BEAR	YOGI		02-11-1950		999999

When selecting a name, it will appear in its own tab titled “Rap Sheet” next to the “Results” tab:



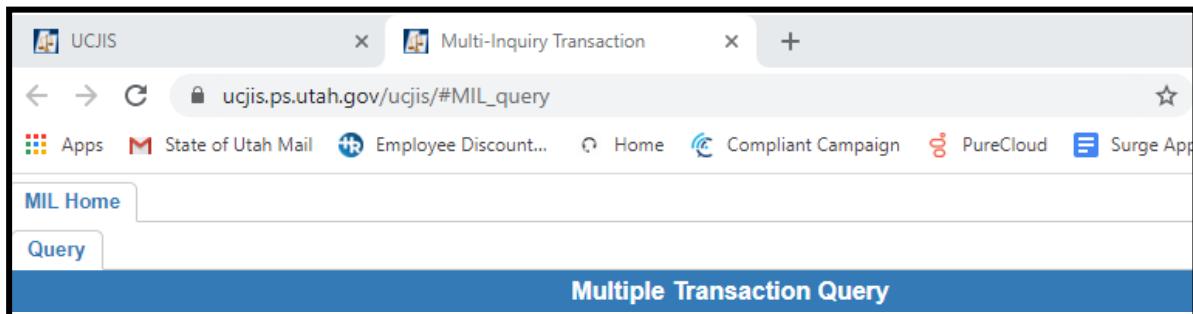
To return to the query results list, click on the “Results” tab. To begin a new query, click on the “Query” tab. All of the previous tabs will remain open until the user closes them.

When selecting names from a DLQ query results list, each name that is opened from the list will also be opened in a new tab. The title of the tab is the name and OLN from the Driver License.



11.2 Multiple Transaction Inquiry (MIL)

Because of the many different files that Multiple Transaction Inquiry opens, MIL opens into a second browser tab next to the main UCJIS browser tab:



After the required information has been entered, the user has the option to specify which files to query at the bottom of the page. By hovering the cursor over any of the transaction titles, a window will appear that explains what is required to acquire information from a specific file.

Transactions to Run	
<input checked="" type="checkbox"/> Driver's License - UTAH (DLQ) <input type="checkbox"/> Criminal History - UTAH (CHQ) <input type="checkbox"/> Drivers License - NLETS (DQ) <input type="checkbox"/> Criminal History - NLETS (IQ) <input checked="" type="checkbox"/> State Wide Warrants (QSW) DLQ - Requires ORI and Name. CHQ - Requires ORI, Requestor Information, and at least one of the following: Name, SSN, or License Number. DQ - Requires ORI, Name, DOB, Sex, and State other than UT. IQ - Requires ORI, Requestor Information, Name, DOB, Sex, Race, and State other than UT. QSW - Requires ORI, Name, and State. QH - Requires ORI, Requestor Information (Right of Access isn't valid), Name, DOB, Sex, and Race. QW - Requires ORI, Name, and DOB. JUV - Requires ORI and Name. OTRK - Requires ORI and Name. MVL - Requires ORI and Name. PO - Requires ORI and Name. ***You can only run transactions you have permission to run.***	
<input type="button" value="Submit"/>	

The Nlets files will only appear if the "State" field has any state other than UT entered:

Transactions to Run	
<input checked="" type="checkbox"/> Driver's License - UTAH (DLQ)	<input checked="" type="checkbox"/> Criminal History - UTAH (CHQ)
<input checked="" type="checkbox"/> Drivers License - NLETS (DQ)	<input checked="" type="checkbox"/> Criminal History - NLETS (IQ)

● MVQL ● QSWL

Home tab. The individual file tabs will have a **green dot** indicating that the response to the inquiry is ready to view. If the color is red, it is not yet ready to view.



● QSWL X ● DLQL X

When a tab has been reviewed, the tab will generate a **red X** and the specific query results will appear in a NAME LIST below:



After selecting a record from the NAME LIST, the record will open in a new tab.



When a different file is chosen, such as DLQ, all of the tabs that were open under CHQ will remain under the CHQ tab, and a new set of tabs will be created under DLQ.

11.3 LOGS Transaction (LOGSL)

The LOGS transaction is used to retrieve a log of the user's inquiries and NCIC entries from the previous 21 days. BCI suggests that no more than five days at a time be requested:

The Audit Logs Results list will appear:

Click on any entry to view the detail. Click on the LOGS tab to return to the results.

If an agency has opened an internal investigation regarding a specific user's usage of UCJIS, the agency TAC or Administrator must contact the BCI Field Services Supervisor for logs that are more than 21 days old.

12.0 Tips and Tricks of UCJIS

BCI will update the Tips and Tricks page as more information becomes available.

TIPS AND TRICKS OF UCJIS	
<ul style="list-style-type: none"> • Google Chrome works best with UCJIS, you can also use Firefox • UCJIS is not case sensitive with the exception of the user's password • Pop-up Blockers should be disabled. This will help especially when having to download or print PC affidavits, eWarrants, UCH, etc. It will also allow you to use Multiple Inquiry transactions such as MIL, VMI, MIP, etc. • UCJIS timeout is set automatically to 30 minutes. Law enforcement timeout is 60 minutes. Contact your TAC or the UCJIS Help Desk if you need to extend your timeout time • LOGS transaction will help you find any transactions you have conducted under your account for the last 21 days • "Windows + L" will lock your computer when you need to step away from your station without logging out of UCJIS • Printing in UCJIS: <ul style="list-style-type: none"> ○ "Ctrl + P" will allow you to print any page you are on ○ CHQ with watermark, select the PDF icon. A new tab will open, be sure pop up blockers are off ○ CHQ without watermark, Ctrl + P ○ Only a certain portion, highlight it then right click and select print • Space Bar will autofill the date and time when entering information in a transaction. It uses the time that is listed on the device that you are accessing UCJIS from. Please ensure that the time on your device is correct • Clear Cache regularly either in the settings or "force refresh" your page by pressing the Ctrl button and clicking the refresh button at the same time 	<ul style="list-style-type: none"> • "500 error" means that there is a problem with UCJIS. Wait a few minutes and then try again • Viewing records click within the line of the record on the query results page to access the record • Querying by SSN will not prefill information if there are more than one name tied to the social security number • Querying by OLN will be the best way to prefill search criteria • UCJIS PIN will be sent to your email when you access UCJIS on a different device. If you are not receiving these emails, ensure that your email is listed correctly on file with BCI. If it is correct and you still aren't receiving the email, have your IT add UCJIS@utah.gov to their receiving email "whitelist" • Transferring an NCIC record to a different ORI can be done with the modify transaction of the type of record. Once the record ORI is modified, a \$O.MOD message will be sent to the new agency to notify them that the record now belongs to them • Keyboard Shortcuts <ul style="list-style-type: none"> ○ Ctrl + (+) key to zoom in ○ Ctrl + (-) key to zoom out ○ Ctrl + P to print ○ Tab to move the cursor to the next entry field ○ Enter to submit a transaction

UCJIS Records



13.0 NCIC Records

Per the Agency User Agreement, each agency acknowledges that quality assurance responsibilities have been developed and approved by the FBI and BCI in order to ensure the legality, reliability, completeness, and accuracy of all records contained in or obtained by means of UCJIS.

Criminal justice agencies agree to maintain records in a timely, accurate, and complete manner. To ensure sufficient record management, BCI affirms that there are security standards, audit standards, and personnel training standards which facilitate accurate record maintenance. Remember, NHELP does not allow periods (.) in entries.

13.1 Responsibility

The primary responsibility for the entry and maintenance of accurate, timely and complete records lies with the originating agency. The "originating agency" is the agency that enters the record under their ORI. Even if another agency (dispatch center, servicing agency) actually creates the NCIC entry on behalf of the originating agency, the originating agency is still responsible for the quality and content of the information.

Any criminal justice agency that relies on another agency to enter information into the NCIC system on their behalf gives that servicing agency authorization to use their ORI to complete the entries. The FBI CJIS division has defined the following areas of quality assurance. For further detail, please refer to the [NCIC Operating Manual](#).

13.2 Accuracy

Any NCIC entry must contain only **correct data**. Agencies should maintain necessary documentation as required by the FBI CJIS policy.

13.3 Completeness

Information contained in an NCIC entry or in a criminal history record must comprise of **all** pertinent, available information. All entries must be 'packed' with all of the information available from other UCJIS files, as well as case files.

13.4 Timeliness

As new information becomes available, the entry, modification, update, and removal of record information must be completed as soon as possible.

13.5 Second-Party Check

The accuracy of NCIC records is an integral part of the NCIC System, the accuracy of a record must be double-checked by a second party, verifying that all accessible files have been reviewed entered into the record.

13.6 Security

Each agency protects its information against unauthorized access, ensuring confidentiality of the information in accordance with laws and the FBI CJIS policy.

13.7 Hit Confirmation

If a participating NCIC agency is not a 24-hour agency, they must be serviced by a 24-hour agency that will monitor and respond to any NCIC hit confirmations in accordance to the policies and procedures set forth by the International Justice and Public Safety Network (Nlets) and National Crime Information Center (NCIC).

13.8 Validation

NCIC validations must be performed on a schedule set forth by NCIC. If not validated in a manner prescribed by NCIC, the entry will be automatically purged from NCIC. All NCIC records must be validated once a year. Validation procedures must be formalized, and copies of these procedures must be on file for review during the BCI or FBI CJIS compliance audits. It is considered a serious compliance issue if an active record is purged by NCIC (\$P) due to lack of validation. Each agency acknowledges that validation is required for the following records: NCIC (boat, license plate, vehicle, gun, securities, persons, selected article files) and statewide warrants and protective orders.

14.0 Nlets

All users in the state adhere to the Nlets policies. All messages transmitted over Nlets must be broadcast in the prescribed message form. Messages with unnecessary verbiage or embellishments damage the integrity of the system. The use of nonstandard abbreviations, as well as criminal and radio codes, must be avoided. Agencies originating want messages of any type (ATLs, BOLOs, etc.) must ensure the cancellation of the messages when they no longer apply. Broadcast messages which are transmitted over Nlets must conform to established guidelines. For further information about Broadcast messages, refer to the Nlets User Policy Manual.

15.0 Statewide Warrants

The use of SWW files is governed by Utah Annotated Code 53-10-207. Every warrant should be comprised of **all** the pertinent, available information. All entries must be 'packed' with all of the information available from UCJIS files, as well as the original case files.

Statewide warrants must be validated per Utah Code Annotated 53-10-208. Statewide warrants that are not validated on a regular basis leave the court liable in the event that a person is wrongfully arrested.

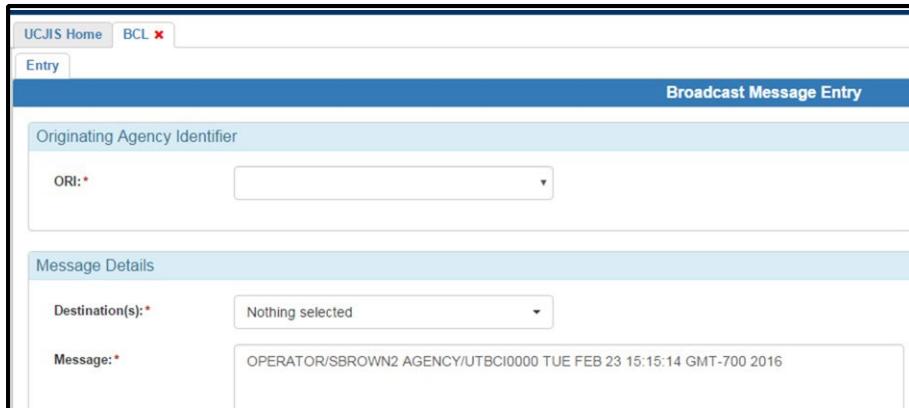
UCJIS Messages



16.0 BCL Transaction

The Broadcast (BC) transaction is a local transaction designed for local agencies to communicate with other Utah agencies. It is a free-text message. Always be professional and specific in the details of the message and include a contact name/number. This is the transaction that is used to send a statewide broadcast message.

BC MESSAGE



The screenshot shows a web-based application for sending broadcast messages. At the top, there are navigation links for 'UCJIS Home' and 'BCL'. Below these are buttons for 'Entry' and 'Broadcast Message Entry'. The main form is titled 'Broadcast Message Entry'. It has two main sections: 'Originating Agency Identifier' and 'Message Details'. In the 'Originating Agency Identifier' section, there is a field labeled 'ORI: *' with a dropdown menu. In the 'Message Details' section, there is a field labeled 'Destination(s): *' with a dropdown menu showing 'Nothing selected'. Below this is a field labeled 'Message: *' containing the text 'OPERATOR/SBROWN2 AGENCY/UTBCI0000 TUE FEB 23 15:15:14 GMT-700 2016'.

17.0 AM vs. BC Messages and YQ vs. YR Transaction Codes

All messages must pertain to official agency matters and investigations. Messages must be as brief and succinct possible.

Administrative Messages (AM) are mostly used for out-of-state messages. An AM message is a criminal justice related agency-to-agency free text message. This message may be asking for information or assistance, or it may be sent in response to a request from another agency. It may be used for any type of information transmission that is not associated with a specific message type. An AM message is intended as a secure and documentable means of interagency communication. Users may send an AM message in response to queries received via phone, fax, radio, or other mode of communication. For more information see the BCI Operating Manual Nlets section, and the Nlets User Policy Manual.

A Broadcast Message (BC) is for messaging inside of Utah. The BC message is a criminal justice related agency-to-agency free text message and should be held to the same standard as AM messages. BC messages can also be sent to specific groups in Utah such as ALLLAW or COURTS. An easy way to remember which message is which is AM could stand for AMERICA and BC could stand for BE HIVE COUNTIES or BE CLOSE messages.

For agencies that enter NCIC records, YQ and YR messages may occur. Users can send a request for a hit confirmation on a record (YQ) to another agency via Nlets. The destination agency will return a hit confirmation response (YR). Although a hit confirmation request relies primarily on the cooperation of the entering agency, the agency making the request should provide sufficient information in the proper format to increase efficiency in the exchange of information.

YQ and YR messages are part of the NCIC Hit Confirmation process sent through the Nlets system. Some of the fields that must be filled in are:

Destination ORI	Who the message is being sent to
Request Type	WP: Wanted Person, SV: Stolen Vehicle, MP: Missing Person, SL: Stolen License Plate, SP: Stolen Part
Request Number	1 for first notice, 2 for second notice, 3 for third notice
Request Priority	U for Urgent, R for Routine

There are two levels of priority provided when requesting a hit confirmation via Nlets: Urgent and Routine. The response time and basis for assignment are described below:

Priority Level:	Priority Code	Response Time	Basis for Assigning Priority
Urgent	U	Within 10 minutes	When the hit is the only basis for detaining the suspect, or the nature of the case requires urgent confirmation of the hit
Routine	R	Within 1 hour	When a person or property is being held on local charges, or when an urgent confirmation is not required

In both cases, a response is defined as either confirming the record or providing a time when the record will be confirmed. For more information, see the BCI Operating Manual Nlets section, the NCIC Operating Manual Introduction section, and/or the Nlets Wiki Page located on the TAC Website.