TAC 101 Packet 2026

December 2025

TAC Responsibilities

The TAC is an agency representative designated by the administrative head of a criminal justice agency. The administrative head, or Agency Administrator, is an individual within a criminal justice agency who has authority over the ORI and may designate duties as well as exercise authority for the agency. The TAC is responsible for their agency's use of the Criminal Justice Information System (CJIS) data. When a new TAC is appointed at an agency, BCI must be notified by the agency administrator by mail, email, or fax. If an Alternate TAC is going to be assigned, the TAC or administrator must notify BCI by mail, email, or fax. The TAC is responsible for making sure all Users, Non-access Users, and Non-Users within their agency have fingerprints submitted to BCI so that the FBI Rap Back system can run daily criminal background checks. If fingerprints are rejected by the FBI for enrollment in Rap Back due to poor quality, a second set of fingerprints must be submitted. If the User's prints are rejected a second time, a name-based search of the FBI's records will be completed and another set of fingerprints must be submitted two years from the submission date of the last set of rejected prints until a set of fingerprints is accepted into the Rap Back system.

*Please note, the Agency Administrator must be set up on the agency's ORI as at least a non-access user or whichever user type is most appropriate.

BCI is responsible for assisting agencies with access to BCI systems. BCI provides the NCIC Operating Manual and NCIC Code Manual, Nlets Manual and the BCI Operating Manuals for these reasons. BCI also offers classroom instruction for training purposes.

The employing criminal justice agency agrees to abide by all present laws, administrative rules, policies, and procedures of CJIS data as adopted by the Utah Legislature and approved by the Commissioner of Public Safety and State Attorney General, as well as any rules, policies and procedures hereinafter adopted and approved. Furthermore, the employing agency agrees to let the TAC train the "recipient" agencies it services on the protection and the integrity of CJIS data by familiarizing the recipient agencies with the laws, rules, policies, and procedures of the system.

The agency also agrees to allow the TAC sufficient time to perform all necessary duties related to CJIS responsibilities, including, but not limited to, attending the annual **mandatory** TAC Conference.

The Utah laws and rules that govern the use of CJIS data are the Utah Code Annotated § 53-10-108 and Utah Administrative Rule R722-900-3.

December 2025

Summary of TAC Responsibilities

- **Dissemination, privacy, security of all UCJIS files**
- **Criminal Justice Agency Agreement**
- **Agency ORI validation**
- **Setting up new users and non-users**
- **Fingerprint Submissions for all Users/Non-users**
- **Creating and deleting logins**
- **User and non-user Security Agreements**
- **Training and testing all users**
- **User Testing Agreements and updating CERT**
- **Updating SAT**
- **Audits – BCI & IT**
- **Policies and Procedures**
- **Validations – $P, $F, ORI, warrants**
- **REPT – keeping it current (names, training dates, etc.)**
- **Attending annual TAC Conference**
- **Training users/non-users after TAC Conference**
- **Passing the annual TAC Test**

Setting up a new User or Non-Access User

Checklist:

- ☐ 1) Provide the user or non-access user with the FBI Privacy Statement Act

- ☐ 2) Add the user into the system using the ADD transaction in UCJIS

- ☐ 3) Fingerprint user using ink ten-print or Livescan
  - Fingerprint all new hires (including POST certified employees and CFP holders)
  - Fingerprint-based background check must be completed prior to granting unescorted access to physically secured locations or activating accounts

- ☐ 4) Fill out **User Setup Form**
  - Use the Google form for Livescan prints
  - For ink ten-print cards, fill out the PDF form and mail it with the fingerprint card to BCI

- ☐ 5) Have the user read and sign the **User Security Agreement**
  - Submit agreement to BCI Field Services

- ☐ 6) Complete CJIS Security Awareness Training **prior to receiving access for all users and non-users** and update their training date using the SAT transaction in UCJIS
  - This does not require a new User Security Agreement to be submitted

* Once the fingerprint-based background check is completed, the User Security Agreement form received by Field Services, and the SAT transaction has been updated, the user's status on agency REPT will be changed to active and the TAC or alt-TAC should assign the user a temporary password with the RSPW transaction

December 2025

- ☐ 7) Complete training and testing **within 6 months** and update the user's training date using the CERT transaction in UCJIS
    - After training and testing, submit the **User Training & Testing Agreement** to BCI Field Services

- ☐ 8) Every year from their hire date, train all user types on CJIS Security Awareness
    - Use the SAT transaction to update their training date

- ☐ 9) Every Two years from their hire date, train and test the user and have them sign a new **User Training & Testing Agreement** and submit the new agreement to BCI Field Services.
    - Use the CERT transaction to update their training date

- ☐ 9) When a user leaves your agency, disable their account using the RU transaction in UCJIS, then submit a **User Deletion Form**.
    - Keep all documents for the user until your agency's next BCI audit (audits are conducted on a 3-year cycle).

**Name-based background checks are not required, however the agency may choose to perform background checks.

If you have any questions, please contact the UCJIS Help Desk or your BCI Field Services Representative (see page 21 for contact information)

New Non-Users

Per Utah Administrative Code Rule R722-900, the definition of a NON-USER is any person who does not have a UCJIS login and has indirect access to criminal justice information from UCJIS. Indirect access is defined as: 1) **unescorted** access to the computer terminal areas where information may be available either on a monitor, printed, verbal **OR** 2) access to computer systems or programs that access UCJIS files.

Non-Users are set up much like Users:

- ☐ 1) Provide the non-user with a copy of the FBI Privacy Statement Act
- ☐ 2) Added to UCJIS using the ADD transaction and check the NON-USER box
- ☐ 3) Submit fingerprints to BCI and fill out the user setup form
- ☐ 3) Train on what is Misuse of UCJIS information
- ☐ 4) Train on **D**issemination, **P**rivacy and **S**ecurity awareness, testing is not required
- ☐ 5) Sign and submit the **Non-User Security Agreement**
- ☐ 6) Update the SAT date after security awareness training is given

Background Checks: Denials

If a User, Non-Access User, or Non-User has a criminal background, BCI must be made aware of it. BCI will review it on a case-by-case basis.

BCI will deny access to UCJIS or UCJIS information on the following reasons (notification will be sent to the TAC and the agency administrator):

- Felony convictions
- Active warrant
- Conviction (or arrest with no disposition) of any severity for:
    - Crimes involving fraud
    - Misuse of UCJIS information
    - Identity theft/fraud

The agency administrator has the opportunity to appeal BCI's decision by submitting supporting police reports, court documents, etc. The agency administrator may also request 'conditional access' if a Memorandum of Understanding (MOU) is in place with BCI which would include a weekly review of the user's logs and increased vigilance.

BCI will grant access on the following closed cases:

- Any Felony: closed 7+ years ago
- Mis. A for Misuse/Fraud: closed 5+ years ago
- Mis. B for Misuse/Fraud: closed 4+ years ago
- Mis. C for Infraction for Misuse/Fraud: closed 3+ years ago

List of TAC Transactions

Located under **Other, LOCAL, TAC Functions**:

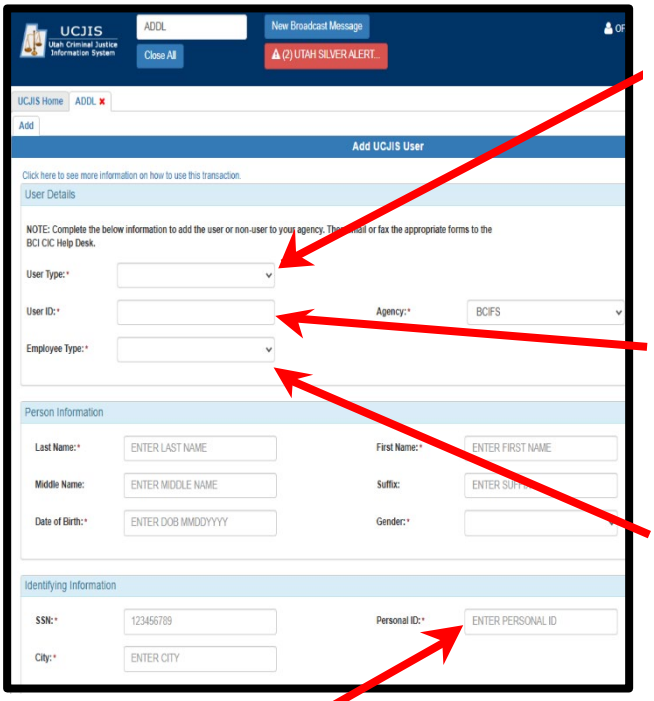
- **ACNT** – Transaction counts by agency
- **ADD** – To add a new User to the agency
- **CERT** – Update User and Non-User training dates
- **MUSR** – To modify User information
- **REPT** - Look at training dates, are backgrounds completed, have fingerprints been received, etc.
- **RSPW** – Reset a User's password
- **RU** – Remove a User's access to UCJIS (before asking BCI to delete them). This transaction will not work if the account is already disabled (doesn't need to happen for non-access users or non-users)
- **SAT** – Update annual Security Awareness Training
- **TCNT** - To view User transaction counts

Located under **Messaging, LOCAL**:

- **BMSG** (Broadcast Messages) - Agency messages, $F, $P
- **LOGS** – To view what Users have been accessing
- **MOTD** – Review previous messages of the day

User/Non-User Functions

Create a login for a new User by completing the **"ADD"** transaction on UCJIS (ucjis.ps.utah.gov):



User Type (choose one)
- User
- Non-Access User
- Non-User

User ID: TAC assigns
- 8 max alpha or numeric
- UCJIS will add 'zz' to non-users

Employee Type:
Drop down, if you select "Other" a free text field will populate to further describe their employee type

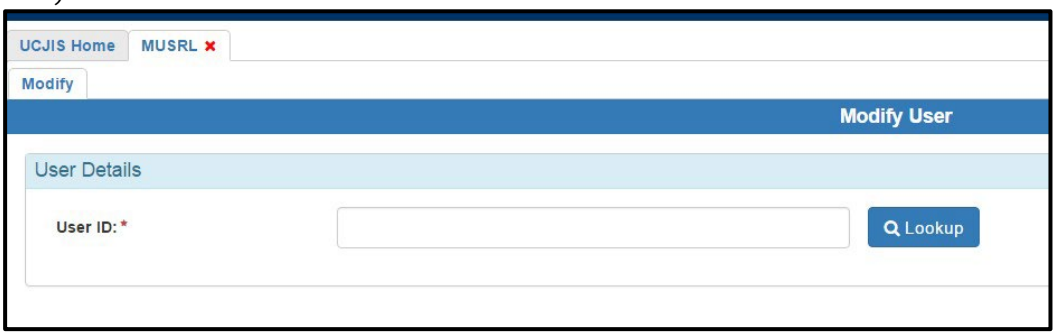
Personal ID:
TAC or User's choice
Use to identify user if they call into the Help Desk

When the login for a USER has been entered, send the **User Setup Form** to the UCJIS Help Desk to activate the login and grant the requested access**.**

**Remember, if you are the TAC for several agencies, you must be set up as a TAC in each agency and keep your User ID and passwords active for each agency.

MUSR (Modify User)

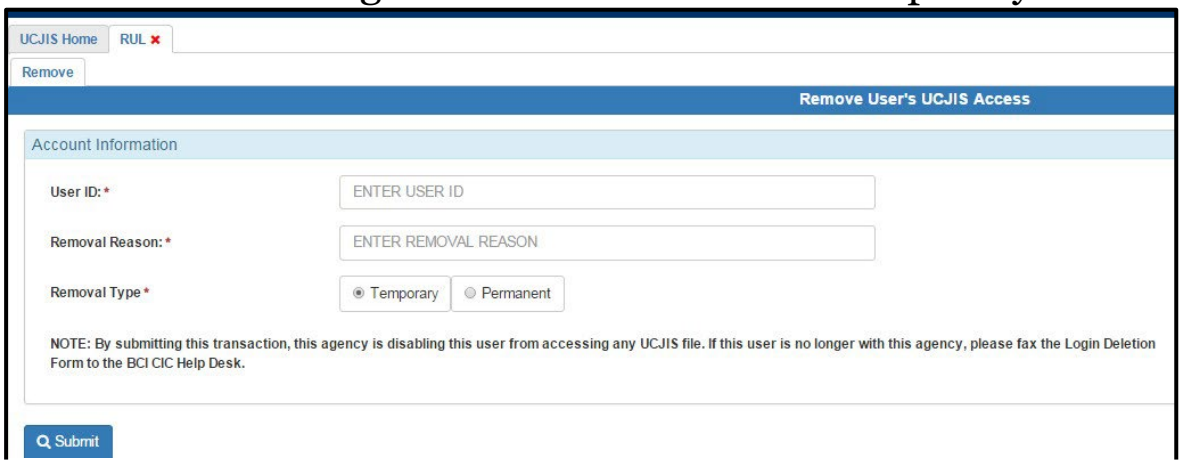
This transaction allows the TAC to update their name, personal ID, and email of all users and non-users.



RU (Remove User)

RU (Remove User) is used to disable a user's account. Please indicate the reason (leave of absence, Military, etc) and select either Temporary or Permanent.

If the User, non-access or Non-User is no longer employed by the agency, the TAC needs to complete a **User Deletion Form** to indicate that the login needs to be removed completely.



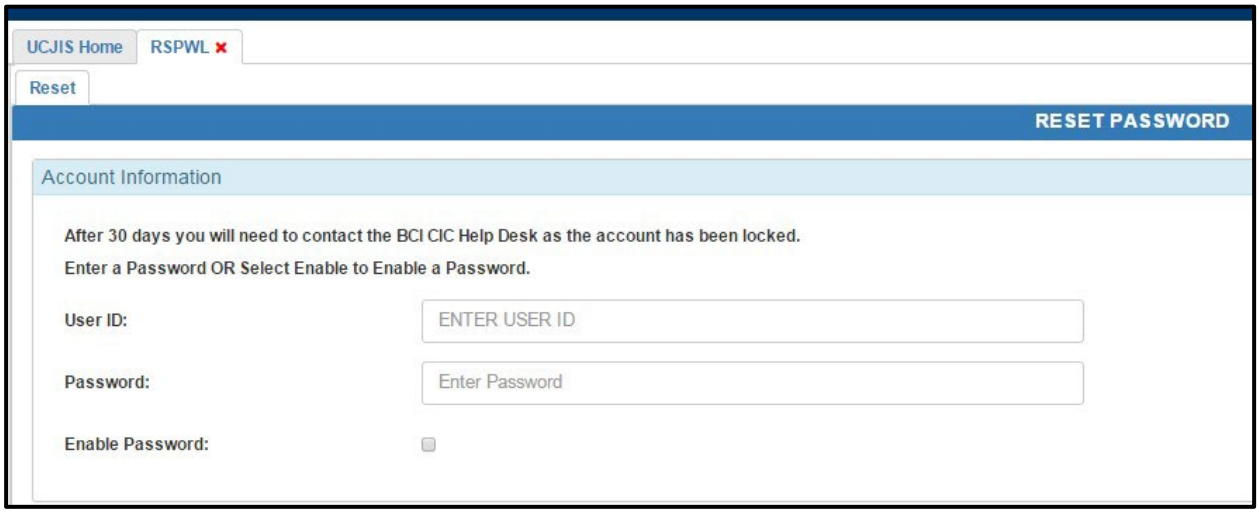
December 2025

Reset or Change Passwords

"RESET" password and "CHANGE" password are not the same thing.

"Reset" password is a function only for TACs or BCI. It allows the TAC to 'enable' the user's current password OR to 'reset' the password by issuing a new temporary password that is only good for three days. Within that three-day time period, the User must log into UCJIS and use the "Change" password transaction (CPW) to create a password that is good for the standard 90 days.

To access the Reset Password transaction, type RSPW into the transaction code field on the UCJIS home page.



Who does the TAC train?

1. All agency Users, Non-Access Users, Non-Users
2. Agencies you service (non-terminal agencies and after hours agencies)
3. Officers and those who receive the information (NonAccess Users, attorneys, clerks, case workers, etc.)
4. Management (Judges, Chiefs, Administrators, etc.)
5. Any authorized persons you give UCJIS information to

What does the TAC train on?

1. Dissemination, Privacy, Security Awareness
2. Accessed Files in UCJIS
3. Misuse of UCJIS information
4. *BCI Operating Manuals and NCIC Manuals*
3. "Message of the Day" (UCJIS Home Page)
4. Information from BCI Newsletters
5. For NCIC entry Users: TOUs (TAC Home Page)
6. What was discussed at the annual TAC Conference

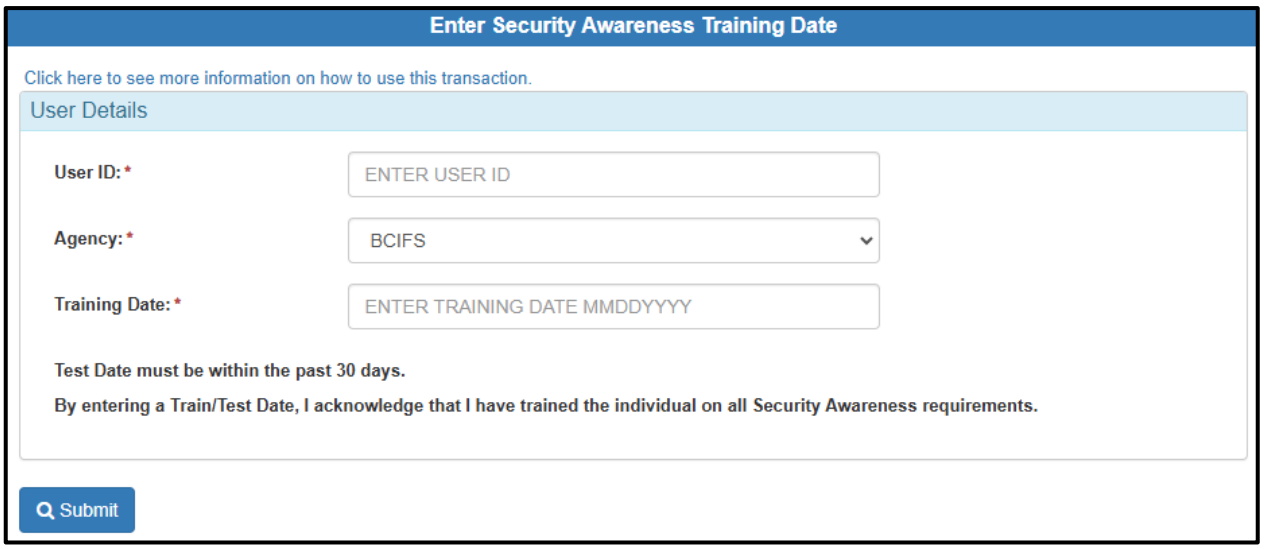
Who does the TAC test?

1. All agency Users (including Non-Access Users)
2. ANYONE who has access to the UCJIS files by way of their personal login ID

SAT
(Security Awareness Training)

The SAT transaction is what the TAC will use to update CJIS Security Awareness training dates for all user types once the training has been completed. The SAT date is what generates the "Security Awareness Training Expiration Date" on the REPT. This date expires on midnight.

Enter the date the training was held. BCI will automatically add one year to this date and this will be their new SAT expiration date.

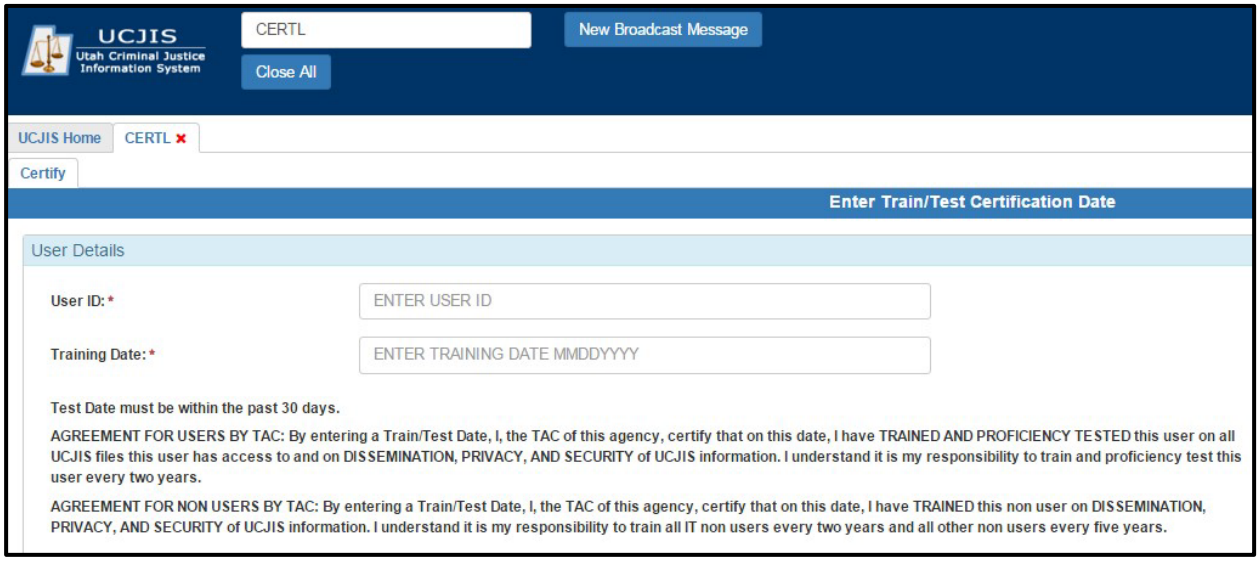


December 2025

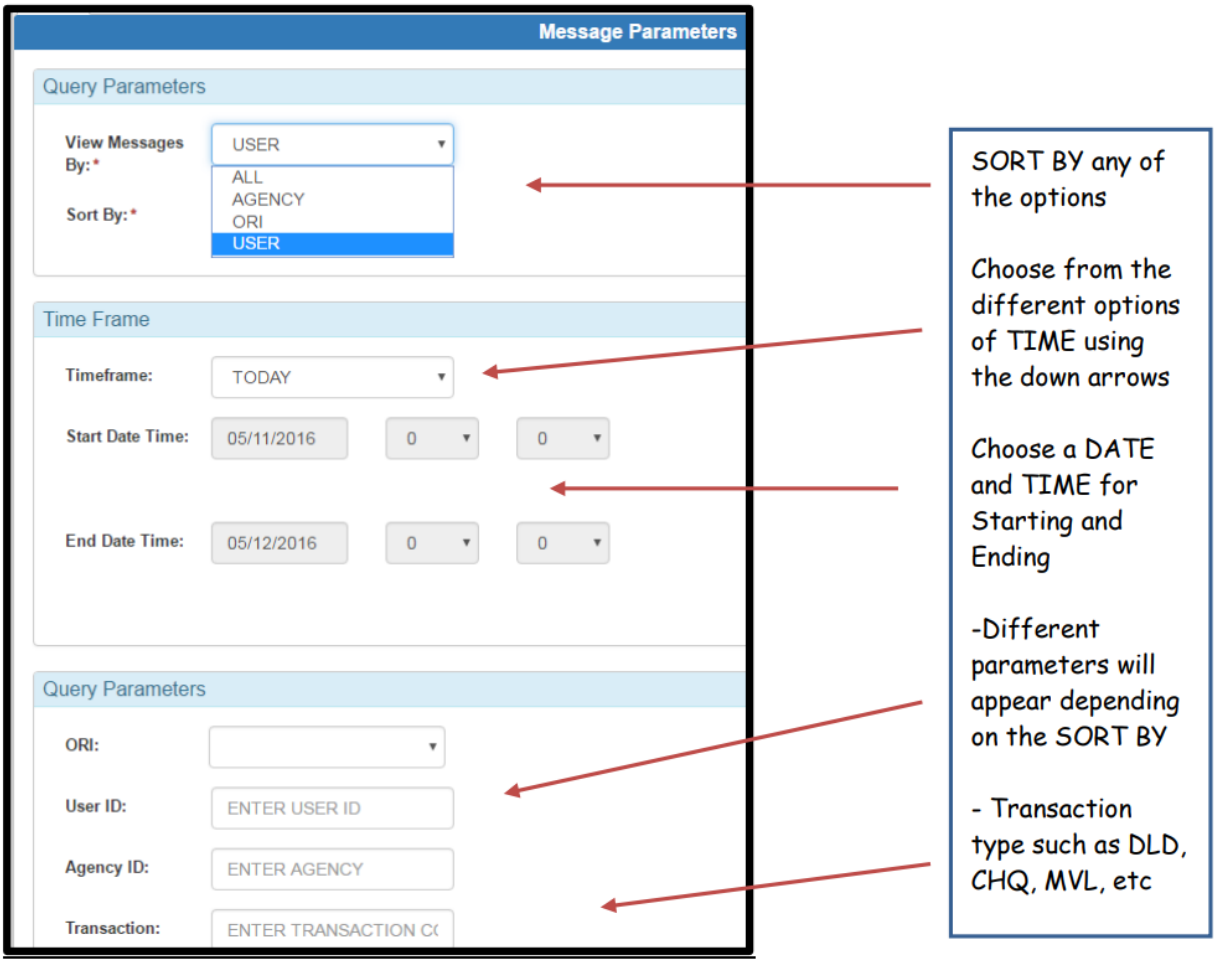
CERT (User Training/Testing)

The CERT transaction is where the TAC must enter the User or Non-User training or testing date when completed. The User must then sign a copy of the "User Testing Agreement" and submit it to BCI. The CERT date is what generates the TRAINING EXPIRES DATE on the REPT Report. The date expires at midnight.

Enter the date that the User signed their Train/Testing agreement into the TRAINING DATE field. BCI will automatically add two years for Users and Non-Users.



LOGS Transaction



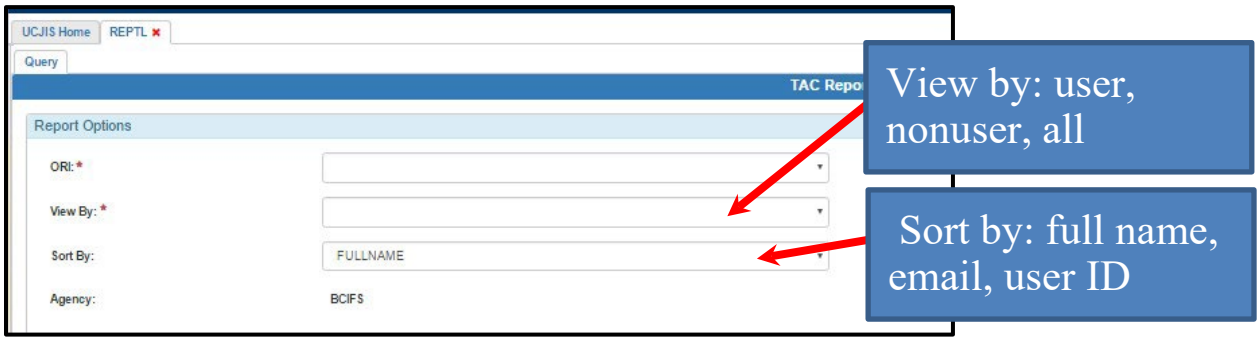
1. Type LOGS into the transaction code field.
2. You can search for all transactions run by the agency or a specific User or by your ORI for agencies who have other agencies accessing UCJIS for them.
3. Information only stays in the LOGS for 21 days. To obtain information older than 21 days, you must submit a **Dissemination Log Request Form**.

**Suggestion: search on small date ranges or search on one specific User by clicking on their user ID on the REPT report.

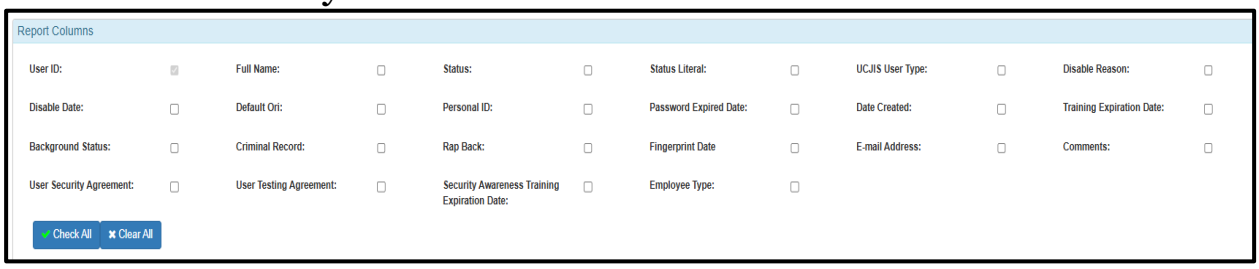
December 2025

REPT Transaction

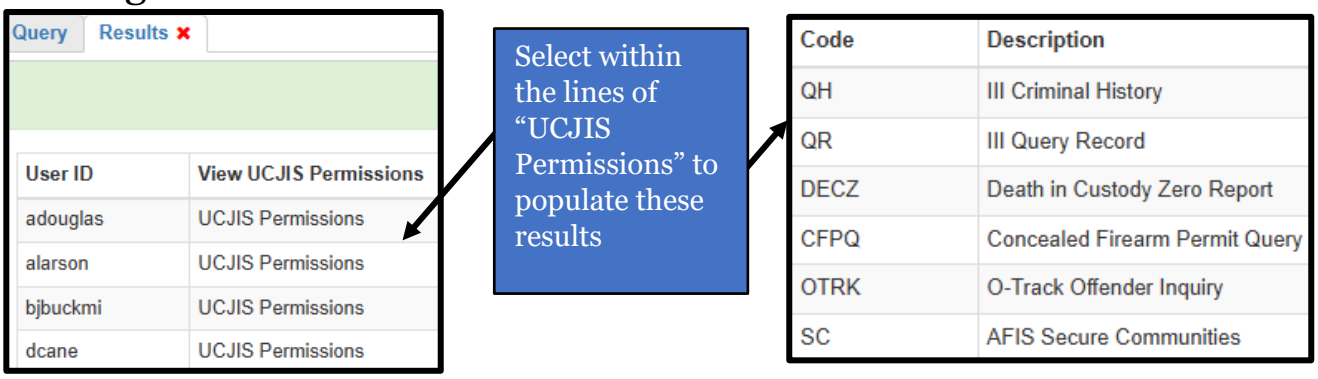
REPT (User List Report Results) allows the TAC to view all User and Non-User information within their agency. Type REPT in the transaction code field. Then choose what type of user you want to see:



Now select what you want to see on the REPT:



TACs now have access to see what files each user has access to by clicking on VIEW UCJIS PERMISSION:



TACs can also view the last 21 days of LOGS for an individual user by clicking on VIEW TRANSACTION HISTORY:

Audit Log Results
Created by ovaisima on 01/15/2025 15:54:52

Received Time	Agency	UserID	Transaction	ORI	Search Fields
01/15/2025 15:29	BCIFS	OVAISIMA	NVAL	UTBCI0000	MONTH=NOVEMBER;QUERY_ORI=UT0291100
01/15/2025 15:27	BCIFS	OVAISIMA	NVAL	UTBCI0000	MONTH=DECEMBER;QUERY_ORI=UT0291100
01/13/2025 10:30	BCIFS	OVAISIMA	NVAL	UTBCI0000	MONTH=JULY;QUERY_ORI=UT0020100
01/13/2025 10:30	BCIFS	OVAISIMA	NVAL	UTBCI0000	MONTH=MAY;QUERY_ORI=UT0020100
01/13/2025 10:28	BCIFS	OVAISIMA	NVAL	UTBCI0000	MONTH=MAY;QUERY_ORI=UT0020100
01/13/2025 10:28	BCIFS	OVAISIMA	NVAL	UTBCI0000	MONTH=APRIL;QUERY_ORI=UT0020100
01/13/2025 10:28	BCIFS	OVAISIMA	NVAL	UTBCI0000	MONTH=MARCH;QUERY_ORI=UT0020100
01/13/2025 10:28	BCIFS	OVAISIMA	NVAL	UTBCI0000	MONTH=FEBRUARY;QUERY_ORI=UT0020100
01/13/2025 10:28	BCIFS	OVAISIMA	NVAL	UTBCI0000	MONTH=FEBRUARY;QUERY_ORI=UT0020100
01/13/2025 10:28	BCIFS	OVAISIMA	NVAL	UTBCI0000	MONTH=FEBRUARY;QUERY_ORI=UT0020100
01/13/2025 10:28	BCIFS	OVAISIMA	NVAL	UTBCI0000	MONTH=JANUARY;QUERY_ORI=UT0020100
01/13/2025 10:27	BCIFS	OVAISIMA	NVAL	UTBCI0000	MONTH=NOVEMBER;QUERY_ORI=UT0020100
01/09/2025 13:28	BCIFS	OVAISIMA	NVAL	UTBCI0000	MONTH=DECEMBER;QUERY_ORI=UT025129E

The REPT also alerts the TAC to when training dates are going to expire OR if they have expired:

Query | Results ✖

User List Report Results
Created by wthomsen on 01/15/2025 16:18:07

User ID	View UCJIS Permissions	View Transaction History	UCJIS Training Expiration Date	User Security Agreement	User Testing Agreement	Security Awareness Training Expiration Date
douglasa	UCJIS Permissions	Transaction History	02-27-2026	No		01-31-2026
alarson	UCJIS Permissions	Transaction History	01-30-2025	No		01-15-2025
cburnst	UCJIS Permissions	Transaction History	01-15-2025	Yes		05-31-2025
dcanet	UCJIS Permissions	Transaction History	06-15-2026	No		01-17-2025
gmcneilt	UCJIS Permissions	Transaction History	08-17-2025	No	05-04-2018	01-15-2025
jdunnt	UCJIS Permissions	Transaction History	02-25-2027	No		01-15-2025
killtest	UCJIS Permissions	Transaction History	05-25-2025	No		01-15-2025
jharr	UCJIS Permissions	Transaction History	12-31-2024	No		01-15-2025
mbiesint	UCJIS Permissions	Transaction History	07-19-2025	No		01-15-2025
mmartinb	UCJIS Permissions	Transaction History	01-09-2020	No		01-15-2025
mmartint	UCJIS Permissions	Transaction History	08-30-2029	No		01-26-2029
ovaisima	UCJIS Permissions	Transaction History	05-24-2025	No		08-06-2025
zztechgy	UCJIS Permissions	Transaction History	08-25-2016	No	N/A	01-15-2025
zztest	UCJIS Permissions	Transaction History	01-19-2025	No	N/A	07-29-2025
wthomsen	UCJIS Permissions	Transaction History	03-31-2031	No		06-19-2025
bear	UCJIS Permissions	Transaction History	02-12-2025	No	04-16-2024	01-15-2026

Training dates that are close to expiring will turn **YELLOW**.
As training dates become expired, the box will turn **RED**.

BCI recommends that TACs run the **REPT** report periodically to ensure that all information on their Users is current and accurate.

What to Expect from a BCI Compliance Audit

BCI Field Services is required to audit each ORI (agency) at least once every three years. The agency administrator and the TAC will receive two emails. One from CJIS Apps and one from Field Services stating it is their turn to be audited and a date as to when the audit information is due. The email(s) will itemize the information that is required:

- Requested documents (Policies, REPT, etc.)
- CASE FILES for requested NCIC records or Statewide Warrants: copy the file and include the original police report
- UCH/III/NLETS LOGS to justify: Please answer all five questions listed in the Audit Information Request form for each log. If the log is highlighted in RED please attach the Right of Access (ROA) waiver.
- Answer the AUDIT QUESTIONNAIRE. If another agency enters your NCIC records, contact them for the answers on the questionnaire. Remember, the ORI on the NCIC record is ultimately responsible for the record and needs to answer the NCIC questions.

December 2025

Documents and Policies Needed for a BCI Audit

Agencies need to have the following documents:

- Misuse Policy that includes the following: "COMMISSIONER and DIRECTOR of BCI will be notified of any misuse as per Utah Code § 53-10-108 (12)"
- NCIC Validation Policy
- Statewide Warrants Validation Policy
- AMBER and EMA procedures: if applicable
- Copies of:
    - REPT- one page only
    - Right of Access (ROA) Contract
    - Right of Access (ROA) Blank Waiver
- Case Files for NCIC entries or Statewide warrants
    - Original police report and signed warrant from the judge through last validation

Validations

Validations should be done on the following:

- NCIC entries
- SWW entries (Courts)

- Monthly Validations must be done 90 days after an NCIC entry has been entered and then annually until the person or item is cleared or cancelled.

- Please make a notation in the case file or somewhere else indicating the monthly validation was done.

- $Fs are NCIC entries that should have been validated last month and were not. If these entries are not validated, the FBI will PURGE THEM ($P) *which is considered a serious NCIC error and will be noted as such on your next BCI Agency audit*.

- $Fs and $Ps are found in UCJIS under the BMSG transaction code and are only available during the first week of the month after the first Saturday of the month.

- Statewide Warrants should be validated as often as possible, AT LEAST once a year.

Contact Information

If you ever have any questions and you can't find the answers, please contact a member of BCI Field Services or the BCI CIC Help Desk.

UCJIS Help Desk: dpscic@utah.gov • 801-965-4446

Field Services Region Representatives:

Region One – Ofa Vaisima: ovaisima@utah.gov • 385-499-1421

Region Two – Scott Williams: scottgwilliams@utah.gov • 385-266-0190

Region Three – Whitney Wilson: wthomsen@utah.gov • 385-499-6963

Region Four – Alena Douglas: amdouglas@utah.gov • 385-499-0186

Region Five – Dylan Cane: dcane@utah.gov • 385-266-1093

Region Six – EmmaLee Sosa • 801-783-6668

Region Seven – Anita Knowley • 801-652-6287

Crime Statistics (UCR/NIBRS/LEOKA):

Alex Martinez: mmartinez@utah.gov • 385-499-5500

Missing Person Clearinghouse/AMBER Alert Coordinators:

Ofa Vaisima: ovaisima@utah.gov • 385-499-1421

Alex Martinez: mmartinez@utah.gov • 385-499-5500

Field Services Supervisor:

Mandy Biesinger: mbiesinger@utah.gov • 801-281-5098