# TAC Responsibilities

# Contents

# Introduction

## INTRODUCTION

The TAC (Terminal Agency Coordinator) program began in Utah in 1985 and was the first such program in the nation. BCI (Bureau of Criminal Identification) has found this program to be the most efficient method for successfully distributing information regarding updates or initiating new procedures and policies governing the use of the Utah Criminal Justice Information System (UCJIS). All TACs and UCJIS users are under the direction of BCI Field Services.

## 1.0 TAC and Alternate TAC Responsibilities

The TAC is an agency representative designated by the administrative head of a Criminal Justice Agency (CJA) and is the liaison between BCI and the Originating Agency Identifier (ORI) agency. Each agency must have a TAC or Alternate TAC (Alt TAC) that is designated to protect the dissemination, privacy, and security, and use of the UCJIS (Utah Criminal Justice Information System) files per the FBI CJIS Security Policy.

When a new TAC is appointed at an agency, the agency administrator must submit a letter, on agency letterhead, to BCI by email. All new TACs shall complete the TAC 101 training provided by BCI Field Services within six months of being designated as a TAC or Alt TAC. An agency may also have as many Alternate TACs as needed. An Alt TAC may have the same access to UCJIS as the primary TAC or limited access to specific TAC responsibilities. The TAC may delegate TAC responsibilities to the Alt TAC. Both the TAC and the Alt TAC must provide the agency with security of UCJIS information when one or the other is out of the office. Both the TAC and the Alt TAC are required to take the annual TAC Tests. To assign a user as the Alt TAC, the primary TAC or administrator must notify BCI by email. If the TAC or Alt TAC leaves the agency or their duties have changed and they are no longer a TAC, please notify BCI of that change.

Throughout this manual, the word TAC is referring to both the primary TAC and Alt TACs.

The agency administrator, by way of the annual Criminal Justice Agency Agreement, agrees to allow the TAC sufficient time to perform all necessary duties and attend mandatory training related to UCJIS responsibilities. It is mandatory for each agency to be represented at the annual TAC Conference by either a TAC or Alt TAC. Those agencies that are not represented risk losing access to the UCJIS files. TACs are responsible for ensuring that changes to existing and introduction of new policies and procedures are trained on and implemented in their agency. The agency administrator and TAC will be responsible for monitoring system use, enforcing system discipline, and assuring that operating procedures are followed by their agency and those agencies they service as outlined in this section under “Agencies with Satellite Offices”. The TAC must have a valid user ID and be certified (trained and tested) annually in order to maintain TAC status.

The agency and TAC agree to abide by all present laws, administrative rules, policies and procedures of UCJIS 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" (criminal justice agencies that receive UCJIS information from an approved UCJIS agency) it serves on the protection and the integrity of UCJIS by familiarizing the recipient agencies with the laws, rules, policies, and dissemination of UCJIS information.

The TAC unifies agency responsibility for system use and serves as a BCI point of contact for record validations, quality control, dissemination of manuals, publications and training materials, security, user access, training, testing, audits, and any other matters concerning the use of UCJIS. TACs are responsible to ensure existing policies are upgraded to current state requirements and the introduction of new policies and procedures are trained on and implemented in their agency. The TAC must ensure that the agency is compliant per the FBI CJIS (Criminal Justice Information Services) Security Policy as far as personnel, physical, and information security is concerned.

BCI Field Services (BCI FS) has the responsibility of operational, technical, and investigative assistance to UCJIS users including training the TAC and providing materials for the TAC and key personnel. BCI FS has the *NCIC Operating Manuals*, *NCIC Code Manuals*, *Nlets Manual*, and *BCI Operating Manuals (AMBER, DLD, DMV, etc.)* available on the TAC Website for all users to access. BCI FS also offers classroom & virtual training for TACs, on-site training at agencies, PowerPoint presentations or documentation to assist the TAC with training their agency.

## 2.0 Agencies with satellite locations throughout the state

Many criminal justice agencies throughout the state of Utah have satellite offices located in several locations throughout the state. Examples of such agencies include the Utah Highway Patrol, Office of Recovery Services, Child Protective Services, Department of Corrections, Department of Child and Family Services, etc.

Although the satellite offices throughout the state perform the same function and are under the same operational umbrella and answer to the same administration, each satellite office is assigned a unique ORI (Originating Agency Identifier) designation by the FBI, and is considered a separate 'agency/ORI' from the other offices under that operational umbrella. For example, the different Highway Patrol sections throughout Utah have offices in different counties, but they all have the same criminal justice function, and answer to the same administrator. Per BCI, each satellite office is considered independent from each other and each office has its own ORI.

## 2.1 TACs at satellite offices

If an agency has satellite offices located throughout the state, an individual at each office must be designated as a TAC for that office/ORI. One individual may be the primary TAC over of the agencies under the same operational umbrella, but an alternate TAC must be in place on-site at each individual office/ORI. If an administrator chooses to designate one primary TAC over all of the satellite offices under the same operational umbrella, that TAC must maintain an active user ID with each of the satellite office/ORI. If an administrator chooses to designate one primary TAC over all of the satellite offices and only that TAC is allowed to attend TAC Conference, the designated TAC is responsible for training the on-site TACs at each of the satellite offices on what was presented at TAC Conference.

## 3.0 Criminal Justice Agency Agreement and ORI Validation

The agency administrator of the ORI is required to sign an annual (July through June) *Criminal Justice Agency Agreement* between their agency and BCI. Failure of an agency to sign and submit the annual *Criminal Justice Agency Agreement* shall be grounds to deny UCJIS access to the agency. If there is a change in the agency administrator, the new administrator must sign a new *Criminal Justice Agency Agreement*. These forms are available on the TAC Website.

Every year, each ORI is required to submit an *ORI Validation Form* updating the agency's address, phone numbers, email address, and the name of the agency administrator, the TAC(s), and IT (computer tech) person. To verify the agency information in NCIC, enter Q0 (Q zero) in the transaction code field in UCJIS. To verify the agency information in NLETS, enter TQ in the transaction code field.

## 4.0 BCI Compliance Audit

As per the *Criminal Justice Agency Agreement*, each agency agrees to be audited by BCI and/or the FBI. This triennial audit is a way of confirming the completeness and accuracy of the information in UCJIS and on the dissemination of UCJIS information. If at any time the TAC or the Administrator has any questions about the compliance audit process, please contact BCI Field Services.

The audit begins with the TAC and administrator being assigned the BCI Compliance Audit through CJIS Apps (Peak Performance). The TAC and administrator will also receive an email from their auditor with the *Audit Information Request, $P messages*, *$F messages*, and *Criminal History Justification Logs*.

After all of the documents have been acquired, please submit them to BCI Field Services by the due date. $P & $F Messages will need to be reviewed and answered in the questionnaire. You will not need to provide documentation for these.

### 4.1 ***Requested Documents:*** **please provide a copy of each of the following:**

- Misuse Policy: Per Utah Statute 53-10-108 (12)(a), the agency Misuse Policy should state that the "commissioner and director of BCI" must be notified if misuse of UCJIS information is suspected OR the policy may say they will abide by Utah Statute 53-10-108.
- NCIC/SWW Validation Policy and Procedures (if applicable): must be in compliance with NCIC and the AOC policies. This includes Felony Warrants.
- AMBER Alert, EMA Procedures (if applicable).
- NCIC Hit Confirmation Agreement: Required if your agency owns records on NCIC and is not a 24 hour agency
- REPT report: submit only the first page of the report.
- Right of Access Waiver Form (if applicable): please provide a blank ROA waiver.
- ROA Contract (if applicable)
- NCIC Case Files (if applicable): copy the entire case file from the original report to the last time it was updated or validated. Please review the NCIC record with the case file prior to submitting the documents to confirm that which is in the case file is noted on the NCIC record.
- Utah Statewide Warrants (if applicable): copy the original document requesting the warrant, the court order issuing the warrant (signed by the judge), and any additional documents pertaining to the warrant.

### 4.2 ***Criminal History Transaction Logs Justification*** **(if applicable)**

Agencies that access Utah Criminal History (UCH) and/or Triple I (III) will be required to justify why the transaction was run. Save the attachment on your computer then you will be able to enter your justification next to each log or print out the attachment and write on each log your answers to the following questions. Please answer the following questions for each transaction:

1) Why was the transaction run?
2) Was the correct purpose code used and if not, what should the code have been?
3) Was the requestor the person who received the information?
4) Is the auditing purpose a case number or specific phrase?
5) And if a log is highlighted in RED indicating a Utah Right of Access inquiry, please provide the signed ROA Waiver Form?

### 4.3 Audit Questionnaire

The *Audit Questionnaire* is currently assigned through CJIS Apps (Peak Performance). You will need to create a Utah ID to access the audit questionnaire. Access will be granted to the TAC and administrator, if your agency would like an Alt TAC to receive the audit instead please notify your Field Services representative.

This *Audit Questionnaire* is 'agency usage' specific. For agencies that have NCIC records, the 'ORI of record' is responsible to answer the questions regarding NCIC entry. Therefore, if your agency has another agency enter your NCIC records, it is still your responsibility to answer the NCIC entry questions which may mean contacting the entering agency to find out their procedures for entering your NCIC entries

## 4.4 Local Agency Security Officer (LASO) Security Audit

The DPS Dept of Technology Services (DTS) will be auditing all agencies that access UCJIS at least once every three years as per the FBI CJIS Security Policy. This audit is to confirm that each agency has sufficient security in place for any computer or mobile device that accesses the secure state wireless network (UWDN). On July 1, 2015, the Mobile Device Management (MDM) was implemented requiring all laptops and mobile devices that access UWDN must be registered with DTS and the agencies must have an MDM policy approved by BCI.

## 5.0 Users (Access and Non-Access) and Non-Users

Per Utah Administrative Rule R722-900, the definition of a **USER** is any person working for or with an agency who has direct access to UCJIS or a person (**NON-ACCESS USER**) who obtains UCJIS records from a person who has direct access. All users must sign a *User Security Agreement* upon being hired.

The definition of a **NON-USER** is any person who **does not** have a UCJIS user ID or direct access to criminal justice information from UCJIS. **Indirect access** is defined as: 1) **unescorted or unrestricted** access to the computer terminal areas where information may be available either on a monitor, printed, or verbal; 2) access to computer systems or programs that access UCJIS files. All non-users must sign a *Non-User Security Agreement* upon being hired.

If you change the user type from a user/non-access user to a non-user or vice versa, you will need to submit a new security agreement to BCI Field Services.

## 5.1 Creating New Users and Non-Users

All UCJIS users must have their own user IDs. Users must never share user IDs, even for training purposes. Each user is responsible for any information accessed under their user ID. It is the TAC's responsibility to create a user ID for each person within the agency that will directly access the UCJIS files. Creating a user ID includes submitting the new user's set of fingerprints and *User Setup Form* to BCI who sends it to the FBI for a fingerprint-based criminal background check. If a TAC, or any user, runs name-based background inquiries on themselves, relatives, neighbors, public personalities, etc. for curiosity, they have committed a Class B Misdemeanor (Utah Code Annotated section 53-10-108) and could be prosecuted.

## 5.2 Background Checks - recertification

Beginning July 1, 2015, if retainable fingerprints (2014+ fingerprints) have been submitted to BCI, then the TAC is not responsible to perform background checks on users or non-users for recertification. The recertification background check is being performed by the FBI Rap Back process. The FBI RAP Back process reviews daily all new arrest prints to the prints already on file with the FBI. If the user or non-user does not have retainable prints, the FBI Rap Back will not work so the TAC must run the background check and submit fingerprints as soon as possible.

### 5.2.1 Denied because of a 'Hit' as per Utah Administrative Code R722-900

If user/non-user has been arrested and a criminal history exists known as a 'hit', BCI automatically denies access to UCJIS unless the charge(s) have been dismissed, declined to prosecute, or acquitted. Access will be granted for any criminal record found with the exception of the following: 1) a felony: pending arrest or conviction; 2) a misuse of UCJIS information charge: pending arrest or conviction; 3) a computer fraud charge: pending arrest or conviction.

The BCI CIC Help Desk Supervisor will email the agency administrator with copies going to the TAC, and the user/non-user to inform them that their access has been denied and explain the appeal process. The user/non-user is in a 'pending' status and will be able to continue to have access to UCJIS for thirty days. During that thirty days, the user/non-user should collect documentation regarding the arrest(s) and give the documentation to the agency administrator. The agency administration submits the documentation to BCI and requests a review. All denied access is reviewed on a case by case basis by BCI after receipt of the letter from the administrator. The exception to this is the severity of the offense which may constitute the user/non-user being disabled immediately with no pending option.

## 5.3 Fingerprints, Retainable Fingerprints, and FBI RAP Back

Effective January 1, 2014, per the Commissioner of the Department of Public Safety, all users and non-users of UCJIS or UCJIS information must have 'retainable' fingerprints on file with BCI. Therefore, if fingerprints were submitted prior to January 1, 2014, a new set of fingerprints will need to be submitted to BCI, this includes all POST and current Utah Concealed Firearm Permit holders. To confirm that BCI has received the retainable prints, view the REPT report. The FBI RAP Back System retains prints for the purpose of being searched by future submissions including latent fingerprint submissions.

Physical ten print fingerprint cards and the *User Setup Form* must be mailed in the same envelope to BCI for all new users and new non-users. New users that are Utah POST certified or have a current Concealed Firearm Permit must also be fingerprinted as of January 1, 2014. If you are submitting the applicant's fingerprints by Live Scan under the B1019 code (law enforcement applicant), mark the Retained Prints on File box on the *User Setup Form.*

The fingerprint card, User Security Agreement and the *User Setup Form* must be submitted to BCI within 30 days of the user ID's creation or the user's UCJIS access will be disabled (FBI CJIS Security Policy 5.12.1 #1). Fingerprints do not need to be re-submitted when a criminal record is found (a 'hit') during the name-based background check if their fingerprints have been received by BCI after January 1, 2014.

## 5.4 Fingerprints when a user leaves one agency for another

If a current user leaves one agency to be employed by a second agency, prior to submitting new fingerprints and a *User Setup Form*, the new agency may want to contact the BCI CIC Help Desk to see if the user has retainable fingerprints already on file. If there are prints on file, there is no need for a new set of fingerprints. The first agency should submit a *User Deletion Form* to BCI. The new agency must submit a *User Setup Form.*

### 5.4.1 Fingerprints taken at BCI

If an agency would like to send their new user to be fingerprinted at BCI, remember to send the user with the *Authorization for Livescan at BCI* form available on the TAC website. Without that form, the user will have to pay for the Livescan prints.

## 5.5 What every User must know

**Dissemination**

- Never discuss information received from any UCJIS file with someone outside of the criminal justice industry
- Even if someone does not have a criminal history and that information is passed to someone outside of the criminal justice industry, that is dissemination and should not be done.

**Privacy**

- Never look up a person in any file in UCJIS for curiosity sake (family, neighbors, ex-family, soon-to-be-family, fellow employees, people you are mad at, people you want to irritate, etc.)
- Never discuss the information you see or print from UCJIS outside of your agency.
- If you misuse the information found in UCJIS, you could be charged with a Class B Misdemeanor.
- If you have visitors at your desk, cover up all information printed from UCJIS and lock your monitor.

**Security**

- Lock your keyboard (the window  key and "L") when you leave your desk.
- Never share User ID information or tell anyone your user ID information and password.
- Retainable fingerprints are checked daily through the FBI Rap Back process for new arrests
- If you print anything out of UCJIS, destroy (cross cut shred or burn) the document when you are finished.

**Manuals**

- Manuals are located on the TAC website, click on MANUALS.
- Open up the manual you need, hit Ctrl F and a search window will appear, type in the word or phrase you are looking for.
- The Operation Manuals tell you how to enter information and what the field acronyms mean.
- The NCIC Code Manuals gives you the codes to enter into the specific fields.

**NCIC Entries**

- Entries must be **accurate, timely, and complete.**
- **"Pack"** the entry with all available information - case files, every file in UCJIS you have access to.

**Courts**

- Entering Jail Release Agreement and Protective Order information timely and accurately is crucial.
- When the Judge makes a decision on a case, enter it into CORIS/UCJIS as soon as possible.
- If the Court does not expire JRA and POs timely, the court may be held liable.
- "**Pack"** a warrant with all available information – case files, every file in UCJIS you have access to.

**Who to call first**

- Your TAC/Alt TAC is the first person you call if you have a problem or need your password reset.
- If your TAC/Alt TAC is not available, call the BCI CIC Help desk: 801-965-4446
- You can also call your agency's BCI Field Services Rep. Click on "BCI Regions" on the TAC website home page to find the name and phone number of your Rep.

**Miscellaneous**

- Passwords expire 90 days from the last time it was set up. If you are on vacation when your password expires, change your password before you leave, type CPW in the transaction code field in UCJIS.

## 5.6 What the TAC needs to do and submit to BCI?

The following must be completed by the TAC for new Users and Non-users:

- *User Setup Form* filled out and submitted to BCI
- Added to UCJIS through the ADD transaction code
- Trained on dissemination, privacy, and security of UCJIS information
- *User or Non-User Security Agreement*: explained and signed
- Users tested on dissemination, privacy, and security of UCJIS information

For new Users and Non-users submitted to BCI:

- *Add to UCJIS*
- *User Setup Form*
- *Fingerprints*: all users, non-access users, and non-users including POST and CFP
- *User or Non-User Security Agreement*
- *User Train and Testing Agreement*

After every TAC Conference:

- Train users and non-users on what was discussed at TAC Conference
- Take and pass the TAC Test (annually)

Annually the following need to be submitted:

- *Criminal Justice Agency Agreement*
- *ORI Validation*

When there is a change in my agency:

- If the Administrator changes, a new *Criminal Justice User Agreement* is signed and submitted
- If a user or non-user leaves the agency, a *User Deletion Form* is submitted to BCI

Every year:

- Train all users and nonusers on security awareness per CJIS Policy 5.2 annually
- Update training date using SAT transaction
- Use a tracker to track security awareness training for agency (optional)

Every two years:

- Train all users on new updates to UCJIS
- Test all users on their proficiency using UCJIS
- Update the users training date in UCJIS using the CERT transaction

## 6.0 Training the Agency Users and Non-Users

The TAC is responsible for training, testing, and affirming the proficiency of users in order to assure compliance with FBI policy and regulations. The TAC is responsible for creating and administering the training and testing for agency users. This training must include, but is not limited to:

- Training on how to access and use the *BCI Operating Manuals* and *NCIC Manuals.*
- Training on dissemination, privacy, and security of the information acquired from UCJIS.
- Training, functionally testing, and affirming the proficiency of all users in order to assure compliance with NCIC policy within six months of employment and biennially thereafter.
- Making appropriate training available for non-sworn criminal justice practitioners, administrators, and upper level managers.
- Provide security and privacy literacy training to all Users and Non-Users
- Providing training for all recipient agencies that the agency services.
- Providing training to TACs at satellite offices.
- Training on *BCI Newsletter* updates what are available to all users
- Training on NCIC TOUs updates for NCIC entries.
- Maintaining records of all training, testing, and proficiency affirmation.

It is required by BCI to keep and maintain records of all training, testing, and proficiency affirmation. These records may be reviewed at the time of the agency compliance audit. All training records and documentation for users, administrative, investigative and enforcement personnel, as well as personnel from recipient agencies must be kept by the agency for at least three years (from compliance audit to compliance audit), even if the user has left the agency. UCJIS misuse issues can arise after an individual has left an agency's employment, and maintaining this documentation can reduce agency liability.

The *BCI Operating Manuals* and *NCIC Manuals* (if NCIC access), must be used to train users. To meet an agency's individual needs, the TAC may develop his/her own training to augment the information the *BCI Operating Manuals.* These manuals are updated on a regular basis. The TAC is also responsible for providing on-going training regarding all updates and enhancements to the UCJIS. *PowerPoint Presentations* on most UCJIS files are also available on the TAC website or from your BCI Field Service Representative. The FBI's website (*www.fbi.gov*) also provides training information.

Training must cover dissemination, privacy, and security of the information accessed through UCJIS, the proper use of the UCJIS files and the types of information available for the performance of the agency's duties. Telling someone that they do or do not have a criminal record is dissemination. Non-users must be trained on dissemination, privacy and security of the information from UCJIS that may be seen or heard. Often the information from BCI pertains to law enforcement activities and **BCI relies on the TAC to disseminate information and training to the officers** that directly or

indirectly access the UCJIS files. Administrators must be made aware of updates and information involved with BCI/FBI CJIS policies, training issues, and new functions made available as these may affect the agency.

## 6.1 Test Records for Training

Users must use approved test records when testing or training on the system. Users are not to run "real" criminal histories or information, even for training unless it is an active case at the agency. Users must never run their own names, even for testing or training purposes. If a user accesses UCJIS to inquire on themselves, family, relatives, neighbors, public personalities, etc. for curiosity or training, that is misuse of the system and is a Class B Misdemeanor (Utah Statute Code 53-10-108) and they could be prosecuted. Another option is to use actual agency cases as part of the training or testing process. Test records for the UCJIS files are found on the TAC website. BCI's test record is Yogi Bear, date of birth 02/11/1950 and can be used in most files for training. Almost all UCJIS files, except Utah Motor Vehicle files, have test records.

## 7.0 Testing the agency Users

The TAC is responsible for creating and administering the training and testing for agency users. Proficiency testing is to be completed within six months of receiving a user ID and every two years thereafter.

## 7.1 FBI Standard

- Within six months of employment or assignment, users need to be trained, functionally tested and affirmation of proficiency must be completed in order to assure compliance with FBI CJIS policy and regulations.
- Provide privacy and awareness literacy training annually and:
  - When required by system changes or within 30 days of any security event for individuals involved in the event
- Provide literacy training and awareness
  - Insider threat
  - Social Engineering
  - Social Mining
- Update literacy training and awareness content annually and:
  - Following any changes in the information system operating environment
  - When security incidents occur or,
  - When changes are made in the CJIS Security Policy
- Use lessons learned from internal or external security incidents or breaches into training and awareness techniques
- Biennially provide functional re-testing and reaffirm the proficiency of terminal (equipment) users in order to assure compliance with FBI CJIS policy.
- Maintain records of all training, testing and proficiency affirmation.

- Initially provide all sworn law enforcement personnel with basic training in NCIC/UCJIS matters to ensure effective use of the system and compliance with FBI CJIS policy regulations.
- Make available appropriate training on NCIC/UCJIS systems for criminal justice practitioners other than sworn personnel.
- Provide all sworn law enforcement personnel and other practitioners with continuing access to information concerning NCIC/UCJIS systems using methods such as roll call and in-service training.
- Provide peer-level training on NCIC/UCJIS systems use, regulations, policies, audits, sanctions, and related civil liability for criminal justice administrators and upper-level managers; and
- Annually review all curriculum for relevancy and effectiveness.

## 7.2 BCI Standard

- Agencies must initially (within 6 months of employment or user ID assignment) train, test, and affirm the proficiency of terminal users in order to assure compliance with FBI CJIS/BCI policy and regulations.
- Provide privacy and security awareness training annually and:
  - When required by system changes or within 30 days of any security event for individuals involved in the event
- Provide retesting every two years to reaffirm the proficiency of terminal users in order to assure compliance with FBI CJIS/BCI policy and regulations.
- Maintain records of all training, testing and proficiency affirmation for at least three years
- TACs (both primary and alternate TACs) will be tested annually by BCI after the TAC Conference. This ensures the TACs have been tested before giving the test to their users (these procedures will be reviewed during the agency compliance audit).
- BCI's minimum standard of training is the *BCI Operating Manual*, *NCIC Operating Manual*, *NCIC Code Manual*, proper dissemination, privacy, and security of the UCJIS and NCIC files.
- Suggested additional training materials could be the *Agency User Agreement, the User Security Agreement* and all other policies and procedures such as the *BCI Newsletter*
- BCI will monitor the testing progress for each agency by the user certification expiration date (CERT date).
- BCI automatically suspends any user if they are not trained and tested by their training expiration date or after their initial six months. If the TAC does not enter the CERT date into UCJIS, the user's UCJIS access will be suspended.
- BCI automatically suspends any user and non-user if they are not trained on security awareness annually by their training expiration date. If the TAC does not enter the SAT date into UCJIS, a user's UCJIS access will be suspended.

- BCI automatically suspends any TAC who did not complete and pass the annual TAC Test by the expiration of their testing date.

BCI and the FBI provide the following resources for training and testing purposes:

- Dissemination, Privacy and Security.
- Available presentations from BCI or the FBI.
- TAC website: training presentations, Manuals, and BCI Newsletters.
- Training offered by BCI for:
  - TAC classes for new TACs, or TACs that want refresher training.
  - TAC Conference.
  - UCJIS Baseline Courses.
  - Specific file training.
- FBI CJIS/BCI policy.
- Statutes that govern UCJIS
- LEEP
- Guidelines on creating agency policies and on creating UCJIS policy

## 7.3 Agency Standard

- The TAC is responsible for the training and testing of all agency personnel that directly or indirectly access UCJIS information.
- Each user must be completely trained on all of the files accessed prior to being tested.
- Each user must only be tested on the files to which access has been granted (i.e., users that do not access NCIC do not have to be tested on NCIC).
- The TAC will create and administer the test for all files that the user is authorized to access. The test can be a practical test, a written test, a verbal test, etc. Each agency will determine the best way to complete the testing of their users. A sample of the test or procedures on how users are tested should be kept on file at the agency.
- The TAC is responsible for updating the user's certification date on the UCJIS website.
- TACs are responsible for the user IDs given to their agency users. Users must be tested by the agency that employs them. Tests are not transferable from agency to agency.
- TACs that fail to certify their users risk losing their UCJIS access pending compliance.

The TAC's training and testing of users should include possible sanctions for misuse. The following concerns should be addressed while creating a training and testing policy and procedures:

- Did the user understand what the agency expected?
- Is the user capable of correctly doing the task that was requested?
- Had the user been previously trained on the areas they were tested on?

- What needs to be done to ensure all users have been functionally trained on any updates?
- How will the agency deal with a user that has failed the test? (i.e. users will be retrained and retested, asked to run a particular transaction and explain the results, etc.)
- What will the agency do if the user fails to comply with those testing policies and procedures set by the agency? (i.e. If a user fails to comply with their agency's testing policies and procedures, access to the system will not be able to continue until the test is taken. The TAC can immediately disable the user's access to UCJIS by the RU transaction in UCJIS.)

## 8.0 User Security Agreement and the User Train and Testing Agreement

Users (access and non-access users) must sign the *User Security Agreement* prior to using their UCJIS user ID. Then within six months of receiving their UCJIS user ID, the user's initial training and testing at the agency must be completed. This agreement does not need to be signed by the user again; it is a one-time document. TACs must submit all *User Security Agreements* to BCI Field Service as per Utah Administrative Rule R722-900-4 and that the original is kept on file for all active users and for at least three years after a user leaves the agency.

Users must sign the *User Training and Testing Agreement* upon completion of their initial training and testing. TACs must submit all *User Training and Testing Agreements* to BCI Field Services as per Utah Administrative Rule R722-900-4. The user must sign and date a **new** *User Training and Testing Agreement* every time biennial re-certification testing is completed and it must be submitted to BCI Field Services.

After the user successfully completes the testing, the TAC must then log into UCJIS and update the user's CERT date. The date on the *User Training and Testing Agreement* and the CERT date should correspond with each other (i.e., the *User Training and Testing Agreement* must be signed on or about the same day the TAC updates the training date using the CERT transaction on UCJIS.)

Agencies must use the agreements provided by BCI. Agreements developed by individual agencies are not considered valid by BCI.

## 9.0 Internal Agency Audits By TACS

TACs must also perform regular internal audits of their agency's UCJIS usage. UCJIS operates under a shared management concept between BCI and system users. Being the point of contact for BCI, the TAC is responsible for the agency's compliance with the *Criminal Justice Agency Agreement* and all policies related to each user. These audits are to include a review of the necessary dissemination, privacy and security practices of UCJIS information, testing and training for UCJIS access, physical and

personnel security, record validation, quality control, dissemination of manuals, policies, and any publications from BCI, audits, and any other matters concerning system use.

Procedures to follow during an internal audit include (but are not limited to):

- Regularly check transaction logs once a week
  - Watch for users running family members, friends, neighbors, public personalities.
  - Watch for users running checks when not scheduled to work.
  - Watch for improper or vague auditing codes and purposes.
- Make sure that agencies with access to your ORI (dispatch centers, etc.) are not improperly using your ORI.
- Ensure that all forms, policies, and procedures are current.
- Have current NCIC and/or SWW validation policies in place (if applicable).
- Make sure secondary dissemination logs are being properly maintained (if applicable).
- Ensure that recipient agencies are being properly trained and audited (if applicable).
- Run REPT transaction to make sure all users and non-users have retainable fingerprints and background checked.
- Ensure your agency is accessing the NCIC TOUs (if you access III and/or NCIC).
- Ensure all paper and electronic media is properly destroyed according to NCIC standards.
- Regularly check the TAC website.
- Complete a security walk-through to ensure that terminals cannot be seen by the public.
- Review what is left on desks at the end of the shift
- Train everyone at the agency who will come in contact with UCJIS information.
- Keep training/testing records three years on all users/non-users including those terminated
- Regularly review the “Message of the Day” on the UCJIS Home Page or from the MOTD code.
- Review AMBER Alert and EMA policies (if applicable).
- Confirm that when discarded UCJIS documents are given to a shredding company in a locked or secured bin to shred or destroy that a user or non-access user witnesses the destruction.

Regularly performed audits find problems, ensure consistent practices, and reduce agency liability. Internal audits can also uncover problems before they get out of hand, and reduce the possibility of user misuse.

## 9.1 What is Dissemination?

In performing an internal audit, the TAC must be aware of what their users are doing with the information acquired from UCJIS and that certain types of dissemination are properly documented. Dissemination means to give out information to other such as:

- UCJIS disseminates information to the user upon the user's inquiry
- A user takes what UCJIS disseminated and gives it to another user
- One agency receives UCJIS information from another agency, that's documented dissemination
- Per the rules of Motion of Discovery, UCJIS information is disseminated and documented
- Past UCJIS dissemination can be acquired from the LOGS transaction or from BCI Field Services

## 10.0 TAC Conference and the TAC Test

All TACs (and Alt TACs) must pass the annual TAC Test administered by BCI. BCI automatically suspends the TACs if the annual TAC Test have not been completed, passed with 80% correct, and the certificate recorded prior to the expiration of their testing date. The annual TAC Test is made available to all TACs after the annual TAC Conference.

The TAC Test is an 'open manual' test. Questions come from the BCI, NCIC, and Nlets manuals, BCI Newsletters, TAC Reminders, any BCI form (all items found on the TAC website). If you are having trouble on a specific question, please call your BCI Field Services Representative.

## 10.1 TAC Conference Attendance and training afterwards

From the *Criminal Justice Agency Agreement* signed each year by the agency administrator: "This agency agrees to allow the Terminal Agency Coordinator (TAC) sufficient time to perform all necessary duties and attend mandatory training related to UCJIS responsibilities. Attendance at the annual TAC Conference is mandatory. Those agencies that are not represented risk losing access to the UCJIS files. TACs are responsible for ensuring that changes to existing and introduction of new policies and procedures are trained on and implemented in their agency". Each agency must be represented at the conference. The TAC or the Alt TAC must attend the conference. It is not necessary for both to be in attendance, but it is helpful so that more of the breakout trainings can be attended.

The TAC Conference is designed to train TACs on new changes from the FBI, legislative changes and updates to UCJIS since the last conference. **It is the TAC's responsibility to train their users after every TAC Conference on the information presented at the conference and complete the TAC Test.**

## 10.2 Did not attend the TAC Conference

If a TAC or Alt TAC is unable to attend TAC Conference, it is their responsibility to acquire the information presented at TAC Conference from either another TAC that did attend or from BCI Field

Services. The TAC is also responsible for training their users on the information presented at the conference and for completing the TAC Test.

## 11.0 TAC Advisory Board

The TAC Advisory Board consists of TACs who have been selected by BCI Field Services. These individuals represent their region to suggest new ideas or report problem areas within the UCJIS files. The agencies that the Advisory Board members work for are typically used for testing new functions prior to the release at the state level. The TAC Advisory Board meets periodically with BCI to exchange ideas, problems and suggestions.

## 12.0 Contact Information

Utah Bureau of Criminal Identification
4315 South 2700 West Suite 1300
Taylorsville, UT 84129
Public telephone number: 801-965-4445
Open Monday through Friday from 8:00 am to 5:00 pm excluding holidays
www.bci.utah.gov

Field Services Manager: 801-281-5022
BCI Field Service Supervisor: 801-281-5098
BCI CIC Supervisor: 385-266-1088
BCI Help Desk (24 hours): 801-965-4446 **for Criminal Justice Agencies Only**
BCI Help Desk email: dpscic@utah.gov

Utah Missing Person Representatives: 385-499-1421 & 385-499-5500
Brady Section Firearm Release: 801-965-GUNS (4867) or 1-800-500-GUNS

Utah Driver License Division: 801-965-3878
Utah Motor Vehicle Division: 801-297-3546

AOC Help Desk: 801-578-3850
NCIC National Help: 304-625-3000 (ET)
NLETS National Help: 800-528-4020
FBI Criminal Justice Information Service: 304-625-4618 (ET)

# Record Validation and Quality Control

# Record Validation and Quality Control

Both NCIC and Statewide Warrant (SWW) records have to be validated on a yearly basis. The primary responsibility for the entry and maintenance of accurate, timely, and complete records lies with the entering agency. The TAC of the ORI on the entry is ultimately responsible for the validations, but can delegate the actual validation process to other individuals in the agency. For information on quality control and validation of specific NCIC entries, please consult the NCIC Operating Manual, Introduction section and individual sections.

## 13.0 NCIC Record Validation

NCIC validations must be performed on a schedule set 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 an FBI CJIS audit. In addition, documentation and validation efforts must be maintained for review during such audit. It is considered **a serious compliance issue** if an active record is purged by NCIC ($P) due to failure to validate.

Validation obliges the ORI to confirm that the record is complete, accurate, and still outstanding or active. Validation is accomplished by reviewing the entry and current supporting documents, and by recent consultation with any appropriate complainant, victim, prosecutor, court, or other appropriate source or individual. Then "pack" the record with as much information as possible, filling in all the fields and adding comments in the miscellaneous field. In the event the ORI is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority must make a determination based on the best information and knowledge available whether or not to retain the entry in the file.

The NCIC records that need to be validated are: wanted/gang member, missing/unidentified person, vehicle/license plate/part/boat. Gun, securities, protection order, sex offender, identity theft, and article.
The VLN field is found in the MODIFY transaction of each record and the name of the user validating the record must be entered into the VLN field. After the record has been validated, only the entering agency will be able to see the name of the validator. For inquiries by other agencies, the VLN field will not appear on the record. To confirm that all records have been validated, the TAC should review the BMSG transaction to see if there are any $F 'Failure to Validate' messages from records that should have been validated last month but were not.

## 13.1 Electronic Validation through UCJIS

NCIC Entries are not considered "validated" unless electronically validated. Entries that are not validated electronically will automatically be purged from the NCIC files. Per NCIC, on the Monday after the first Saturday of the month NCIC sends BCI the NCIC entries that need to be validated. BCI makes these files available through UCJIS in the NVAL transaction for each agency to retrieve. BCI

puts a notification on the UCJIS "Message of the Day" when the entries are ready to be retrieved. TACs should make it a habit to always check the NVAL transaction on the Monday after the first Saturday of every month. These entries must be electronically validated during the current month through the MODIFY transaction of each file.

If a record has not been validated within a month from the request for validation, the NCIC System will generate a $.F. Failure to Validate Notification to the ORI on the Monday following the first Sunday of the month. The $.F. notification serves as a warning for the agency to validate the record or the NCIC System will retire the record during the next purge cycle. If the record is not validated by the first Sunday of the following month, the NCIC System will retire the record and generate a $.P. Purge Failure to Validate Notification. Receiving a $P entry is considered a serious NCIC error and it will be noted as such on the next agency audit.

### 13.2 NVAL for monthly validations

Monthly validations are accessed through UCJIS using the NVAL transaction on the first Monday following the first Saturday of the month. If you are having problems accessing your monthly validations, please contact your BCI Representative. These validations will be available for exactly one year.

### 13.3 $F Failure To Validate

BCI recommends that each month the TAC double check in UCJIS to make sure that all of their NCIC entries from the previous month have been validated. This can be accomplished by entering the message type of $F in BMSG after the first Saturday of the month. To see if there are any NCIC records that should have been validated last month ($F records), enter into the transaction code field BMSG. If a log appears, click on the log and the entire entry will appear. Print out the entry and validate it as soon as possible.

## 14.0 Statewide warrant validation – Court responsibilities

Statewide warrants must be validated yearly per Utah Code Annotated 53-10-208. Statewide warrants that are not validated on a regular basis leave the court open to liability in the event that the wrong person is arrested based on the information in the warrant, or in the event that an arrest is never made based on the poor quality of information in the warrant.

Entries into the Statewide Warrant file need to be complete and accurate. This increases the chances of the defendant getting arrested and decreases the court's liability in the event of a false arrest.

According to state and federal law, individuals with outstanding warrants, active protective orders, felony convictions, or domestic violence convictions, cannot possess firearms (the domestic violence

conviction does not have to be a felony to prevent possession of a firearm). If the law enforcement agency performing the background check on the purchaser cannot prove that he/she has disqualifying incidents in their background check, the firearm must be sold to that person.

In order to ensure the accuracy of the SWW files, entries need to be validated. Utah Code Annotated 53-10-208 specifies that validation checks must be completed on a regular basis. The law states:

> "(3) The division [BCI] is the agency responsible for the statewide warrant system and shall: (a) ensure quality control of all warrants of arrest or commitment and protective orders contained in the statewide warrants system by conducting regular validation checks with every clerk of a court responsible for entering the information on the system."

To verify information, the court must obtain a listing of all warrants that are entered into the system using its court ID and a listing of all warrants entered by the court that have been placed into the "served" status by law enforcement agencies (Booking Report). The Booking Report is emailed to the court from the AOC.

Warrants must be reviewed on a regular basis; therefore, the agency needs to develop validation procedures for the individual court. These must be formalized and on file at the agency and at BCI. When the agency is audited by BCI these procedures will be reviewed.

Courts must use any UCJIS file available to them to gather information about the defendant. If the defendant has a valid Utah driver license, this will usually contain all required information. However, any other UCJIS file can be used when necessary. This includes UCH, SWW, III, Nlets, NCIC, juvenile files, the jail connect files, OTRK, MVD, etc. Then "pack" the record with as much information as possible, filling in all the fields and adding comments in the miscellaneous field. Courts can also use information in their own files, or contact the arresting agency or prosecuting agency. It is very important that the record is 'packed' with all available information.

## 14.1 CORIS and SWW

Courts use the CORIS software system to download warrants on to UCJIS. CORIS is a direct interface into UCJIS. What a court enters into CORIS is seen immediately by agencies accessing statewide warrants through UCJIS, or through any other software vendor.

Any court in Utah can access the UCJIS files. Courts that currently cannot access the UCJIS files can request access through BCI. The UCJIS files should be used to gather identifying information to enter into the warrant, and also to update and validate the warrant as time goes by.

## 15.0 Quality Control - NCIC

As stated in the *NCIC Operating Manual*, *Introduction section*, "agencies that enter records in NCIC are responsible for their accuracy, completeness, timeliness, security, and dissemination." This requires a second party check on entry, add-on, modification, cancel and clear transactions. The second party check needs to be performed by a person other than the User that executed the original transaction. This can be the TAC or any other person designated by the TAC. The second party check is used to ensure that the NCIC record contains the most complete and accurate information possible.

The *NCIC Operating Manual's* definitions are:

- ACCURACY: The agency must take appropriate action to ensure the accuracy and completeness of the NCIC record as part of the second-party check process.

- COMPLETENESS: Complete records include all critical information that was available on the person or property at the time of entry. Critical information is defined as data fields that will: (1) increase the likelihood of a positive hit on the subject or property and aid in the identification of a subject or property; or (2) assist in compliance with applicable laws and requirements.

- TIMELINESS: Entry, modification, update, and removal of information are completed as soon as possible after information is available and information is processed and transmitted in accordance with established standards. NCIC records must be entered immediately when the conditions for entry are met, not to exceed 3 days, upon receipt (electronic or hard copy format) by the entering agency. The only exceptions to immediate entry are when otherwise prescribed by federal law or when documentation exists to support delayed entry.