Introduction File

Table of Contents

2.9.4 NICS ADMINISTRATIVE MESSAGES

2.9.4.1 $.NICS.DOWN NICS Out-Of-Service Notification

A $.NICS.DOWN NICS Out-Of-Service Notification is transmitted to all NICS users when NICS is going out of service. Up to 80 characters of text can be inserted in the free text message.

```
$.NICS.DOWN.
NICS GOING DOWN


NICS OUT OF SERVICE UNTIL <hhmm> EST
```

2.9.4.2 $.NICS.UP NICS Return-to-Service Notification

A $.NICS.UP NICS Return-to-Service Notification is transmitted to all NICS users when NICS is returned to service.

```
$.NICS.UP.
NICS IN SERVICE AT <hhmm> EST
```

3 QUALITY CONTROL, VALIDATION, AND OTHER PROCEDURES

3.1 MAINTAINING SYSTEM INTEGRITY

The primary responsibility for the entry and maintenance of accurate, timely, and complete records lies with the entering agency. However, the CJIS System Agency (CSA) assumes a large degree of administrative responsibility, and possible legal liability, for the maintenance of a criminal justice information system. This responsibility is being further defined by the courts. Accordingly, the CSA should institute appropriate and reasonable quality assurance procedures for all federal and state System users. It appears from the cases reviewed that the courts have specifically addressed the issue as to whether criminal justice information system administrators (i.e., CTO, CSO, or agency head) can be held liable for the negligent mishandling of a criminal justice record. In relation to Title 42, United States Code 3771, there is a standard which is prescribed for record management and, perhaps, the establishment of maintenance standards for these records. Criminal justice agencies specifically have a duty to maintain records that are accurate, complete, and up-to-date. To ensure reasonably sufficient record management, for electronic and/or hardcopy case management systems, each CSA should ensure that there are security standards, audit standards, and personnel training standards which allow accurate and up-to-date records and proper/secure dissemination of the same. The following standards have been established and approved by the CJIS APB with regard to security, audit, and training:

3.1.1 Security

Security standards are documented in the CJIS Security Policy. The CJIS Security Policy includes personnel, physical and technical security, as well as user authorization and dissemination.

3.1.2 Audit

All federal and state CSAs shall establish a system to triennially audit every terminal agency that operates workstations, access devices, mobile data terminals, or personal/laptop computers to ensure compliance with state and FBI CJIS policy and regulations.

In addition to audits conducted by all CSAs, each federal and state CSA shall be audited at least once every three years by the FBI CJIS audit staff. This audit shall include a sample of state and local criminal justice agencies. The objective of this audit is to verify adherence to FBI CJIS policy and regulations and is termed a compliance audit. In order to assist in this audit, each CSA will respond to a preaudit

questionnaire which will serve as the audit guideline. A compliance audit may be conducted on a more frequent basis should it be necessary due to failure to meet standards of compliance.

Such compliance audits shall cover the following areas in connection with both the NGI/III and NCIC property and person records:

3.1.2.1 Accuracy

Any NCIC entry should contain only correct data. In addition, CSAs should maintain necessary documentation as required by FBI CJIS policy. They should also ensure that documentation is available from state and local users accessing NCIC through them

3.1.2.2 Completeness

Information contained in an NCIC entry or in a criminal history record to be disseminated is comprised of all the pertinent available information.

3.1.2.3 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 standards as established by the APB.

3.1.2.4 Security

An organization protects its information against unauthorized access, ensuring confidentiality of the information in accordance with laws and FBI CJIS policy, regulations, and standards.

3.1.2.5 Dissemination

All information released is in accordance with applicable laws and regulations, and a record of dissemination of criminal history records is maintained.

In addition, CSAs should ensure that documentation is available from local users to assist in triennial state and federal audits.

3.1.3 Training

CSAs must:

1. Within 6 months of employment or assignment train, functionally test, and affirm the proficiency of terminal (equipment) operators in order to assure compliance with FBI CJIS policy and regulations;
2. Biennially, provide functional retesting and reaffirm the proficiency of terminal (equipment) operators in order to assure compliance with FBI CJIS policy;
3. Maintain records of all training, testing, and proficiency affirmation;
4. Initially (within 12 months of employment or assignment) provide all sworn law enforcement personnel with basic training in NCIC matters to ensure effective use of the System and compliance with FBI CJIS policy regulation;
5. Make available appropriate training on NCIC System use for criminal justice practitioners other than sworn personnel;
6. Provide all sworn law enforcement personnel and other practitioners with continuing access to information concerning NCIC /state Systems using methods such as roll call and in-service

training;

7. Provide peer-level training on NCIC System use, regulations, policy, audits, sanctions, and related civil liability for criminal justice administrators and upper-level managers; and

8. Annually review all curricula for relevancy and effectiveness.

3.2 MAINTAINING THE INTEGRITY OF NCIC RECORDS

Agencies that enter records in NCIC are responsible for their accuracy, timeliness, and completeness. The FBI, as manager of the NCIC System, helps maintain the integrity of the system through:

1. Automatic computer edits which reject certain common types of errors in data (edit instructions appear in each chapter of this manual where applicable),

2. Automatic purging of records after they are in a file for a prescribed period of time (retention instructions appear in each chapter of this manual where applicable),

3. Quality control checks by FBI's Data Integrity Staff, and

4. Periodically furnishing lists of all records on file for validation by the agencies that entered them. This section addresses quality control and validation procedures.

Electronic Records Management System (ERMS) Note:

An ERMS is defined as any electronic database, including an electronic warrant database. Agencies must conduct appropriate follow-up to resolve discrepancies identified during synchronization and cross-checks. All electronic processes must be approved and accepted by the CJIS Systems Agency and be in compliance with CJIS security and NCIC policies. Compliance with CJIS and NCIC policies may be achieved through electronic or manual processes.

Examples of ERMS processes include:
- an agency enters the original information directly into ERMS without paper.
- an agency completes a hard copy document, scans or enters the document into an ERMS, performs a second-party check from the original hard copy, and destroys the hard copy. All modifications are done on the ERMS.
- an agency completes a hard copy document, scans or enters the document into an ERMS, performs a second-party check from the original hard copy, and places the original copy in storage for historical purposes only. All modifications are done on the ERMS.

In all cases, the information in the ERMS is considered the source document.

3.2.1 Accuracy

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.

The verification of a record should include assuring all available cross checks, e.g., VIN/LIC, were made and that the data in the NCIC record match the data in the investigative report.

Note: For ERMS, electronic synchronization and cross-checks are an acceptable process to ensure the integrity of the NCIC. The synchronization and cross-checks must compare the electronic record with the NCIC record to identify additional or inaccurate information. The agency must take appropriate action to ensure the accuracy and completeness of the NCIC record as part of the second-party check process. If the agency's ERMS searches other databases or systems, such as the Department of Motor Vehicles

(DMV), court records, or the Next Generation Identification (NGI) Interstate Identification Index (III) to populate its NCIC records, the second-party check must also include a file synchronization against the other sources checked, e.g., DMV, court, or NGI/III, and appropriate follow-up to resolve discrepancies to ensure the accuracy and completeness of the NCIC records.

For an ERMS and prior to a data transfer process being implemented, the process must be thoroughly tested and verified, via a "record-to-record" and "field-to-field" comparison, for the accurate and complete transfer of the data to the NCIC. Once tested, verified, and trusted, periodic synchronizations, to occur at least annually, between the ERMS and NCIC are required to identify errors that may have occurred in the transfer process. Synchronizations must also occur after software and/or hardware upgrades and/or system maintenance. Front end testing and verification is a requirement to allow a system to system data transfer to serve as the second-party check on the transferred data from the ERMS to NCIC.

3.2.2 Timeliness

To ensure maximum system effectiveness, 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.

- **Wanted Person File** -- Entry is made immediately after the decision to arrest or authorize arrest has been made.

  Before entering a wanted person record in NCIC, the entering agency must attempt to determine, to the maximum extent possible, if extradition will be authorized if the individual is located in another state. In situations where an agency is absolutely certain that the wanted person will not be extradited, the individual's record may be entered in NCIC indicating no extradition, using the Extradition Limitation (EXL) Field. Also, if there is a limitation concerning extradition of the wanted person, such information should be entered using the appropriate code in the EXL Field . In instances where an ORI will not honor the extradition of an individual, the ORI must initiate a modify message to update the extradition limitation appropriately. Although all records may be entered into the NCIC Wanted Person File, extradition must be addressed prior to entry so that appropriate extradition information can be included in the record.

- **Federal Fugitive Records** -- Entry is made immediately (i.e., within 24 hours) upon receipt of information by the inputting agency/office, after the decision to arrest or authorize arrest has been made.

  Exceptions to this rule occur if imminent arrest is expected or other clear, identifiable, operational reasons would preclude immediate entry (e.g., insufficient descriptive data resulting in a "John Doe" warrant). Any exceptions to delayed entry in NCIC must be minimized and documented.

- **Missing Person File** -- Entry is made as soon as possible once the minimum data required for entry (i.e., all mandatory fields) and the appropriate record documentation are available. For missing persons under age 21, an NCIC Missing Person File record should be entered within 2 hours of receiving the minimum data required for entry.

- **Article, Boat, Gun, License Plate, Securities, Vehicle/Boat Part, and Vehicle Files** -- Entry is made as soon as possible once the minimum data required for entry (i.e., all mandatory fields) and the record documentation are available. Information about stolen license plates and vehicles should be verified through the appropriate motor vehicle registration files prior to record entry if possible. However, if motor vehicle registration files are not accessible, the record should be entered into NCIC and verification should be completed when the registration files become available.

- **All other files** -- Entry is made as soon as possible once the minimum data required for entry (i.e., all mandatory fields) and the appropriate record documentation are available.

Additional explanations of "timely":

- Modifying, clearing, locating, or canceling a federal fugitive's NCIC record should occur immediately (i.e., within 24 hours) upon receipt by the inputting agency/office of the information prompting the change.
- **Timely modification** of a record is that which occurs as soon as possible following the detection of erroneous data in an existing record and as soon as possible following the receipt of data not already stored in the record.
- **Timely inquiry** requires that the transaction is initiated before an officer begins writing an arrest or citation document of any kind; inquiries are stored when NCIC is not available and submitted at once when the System returns, regardless of whether the subject is still in custody; inquiry is made prior to release of a person who has been incarcerated; and inquiry is made upon those who appear at a custodial facility to visit inmates.
- **Timely entry** of a locate is that which occurs as soon as reasonably possible once the record in question has been confirmed with the originating agency.
- **Timely removal** from the file requires immediate removal of the record once the originating agency has documentation that the fugitive has been arrested or is no longer wanted unless being detained.

3.2.3 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. Validation should include a review of whether additional information which is missing from the original entry that could be added has become available for inclusion to the record.

Complete inquiries on persons include numbers, i.e., Social Security number, passport, vehicle identification number, license plate, driver's license, etc., that could be indexed in the record. Inquiries should be made on all names/aliases used by the suspect. Complete vehicle queries include vehicle identification number and license plate numbers.

3.3 QUALITY CONTROL

FBI CJIS personnel periodically check records entered in the System for accuracy. Errors discovered in records are classified as serious errors or nonserious errors. This classification determines the type of action that is taken by FBI CJIS.

3.3.1 Serious Errors

- Wanted Person File records which indicate that the subject is wanted for questioning only.
- Records entered for cashier's checks, bank drafts, bank officer's checks, certified checks, checks issued to card holders by credit card companies, company checks, government checks (local, state, and federal), personal checks, personal notes, and promissory notes.
- Records entered for stolen credit cards.
- A missing person, wanted person, license plate, or vehicle record containing inaccurate vehicular and/or license data that has been verified as inaccurate by the State Department of Motor

Vehicles (DMV) where the vehicle is registered or by comparison with VIN specifications obtained from the manufacturer.

Such inaccuracies can be uncovered when the state of registry compares license and vehicular data in the NCIC $.8. message with records contained in its DMV Files. Upon discovery of inaccurate data, the state of registry should advise the ORI of the error. If the ORI fails to correct the error within a reasonable period of time, the state of registry should notify FBI CJIS. The entry of incorrect data in the LIC, License Plate Year of Expiration (LIY), or VIN Fields will be considered a serious error. Incorrect data entered in any of these fields might lead to a false arrest or possibly more serious consequences. On notification from the state of registry, FBI CJIS will cancel a Vehicle or License Plate File record which contains inaccurate information in the LIC, LIY, or VIN and will delete the inaccurate vehicular and/or license data from a Wanted or Missing Person File record.

- Records entered in the wrong file.
- Property records entered with a nonunique number such as a stock number, model number, an owner applied number in the SER Field, a nonunique boat hull number, or nonunique boat registration number, etc.
- Property records entered with generic codes which do not have the manufacturer's name or other identifiable data in the record.

3.3.2 FBI CJIS Procedures for Errors

In connection with maintaining the integrity of NCIC records, each state control terminal agency should continue to develop and maintain stringent quality control procedures to ensure that all records in NCIC are kept accurate, complete, and up-to-date.

3.3.2.1 Serious Errors

- In cases of serious errors, FBI CJIS will cancel the record and transmit a $.E. administrative message to the entering agency. The $.E. message provides the entire canceled record and a detailed explanation of the reason for cancellation.
- Assumption of this limited responsibility for cancellation of a user's entries in connection with the foregoing quality control procedures does not make the FBI the guarantor of the accuracy of NCIC records. The ORI is responsible for the accuracy, completeness, and current status of its records entered in NCIC.

3.3.2.2 Nonserious Errors

- A nonserious error is by definition an error found in any NCIC record which is not covered by the above serious error list.
- When a nonserious error trend is discovered, FBI CJIS will mail a letter to the appropriate CSA. The CSA will forward a copy of the letter or a similar letter to the agency originating the record so corrective action can be taken. No further action will be taken by FBI CJIS.

3.4 VALIDATION

- 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, nonterminal agency, or other appropriate source or individual. 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.

Note: The current supporting documents may be electronic or hard copy if the CSA and the originating agency recognize the document as official. Also for electronic warrant systems, checking the appropriate source to see if the warrant is still active may be accomplished by using an ERMS. For ERMS, the CSA and the originating agency should ensure additional checks and balances are in place to verify the validity of the systems, i.e., files must be synchronized with the appropriate sources/systems being used. The comparison must identify records that are non-existent in one or more of the synchronized databases and the agency must conduct a follow-up to resolve discrepancies. For valid records, the synchronization must also compare the electronic record with the NCIC record to identify additional or inaccurate information. If the agency's ERMS searches other databases or systems, such as the DMV, court databases, or the NGI/III, to populate its NCIC records, the monthly validation must also include file synchronization against the other sources checked and follow-up to resolve discrepancies to ensure the accuracy and completeness of the NCIC records.

- Each month CSAs receive a file of records to be validated. The CSAs in turn distribute the records to be validated to the ORIs as appropriate. On the first Saturday of the month, the NCIC System selects the records scheduled for validation. The NCIC System does not retrieve for validation those records that have been validated within the last calendar month.

  The CSA selects to conduct validations on-line or to notify CJIS that validations have been completed.

  If a state/federal agency uses the **on-line validation process**, the agency must modify each record being validated to include updated information in the Name of Validator (VLN) Field. 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.

3.4.1 Validation Schedule

- On a monthly basis, the NCIC System extracts active records on file for validation purposes. The validation includes a portion of each file and includes those records 60-90 days old. In addition, it includes any records 14-15 months old, 26-27 months old, 38-39 months old, etc. The validation schedule is as follows:

  Validation: Entries Made on:

  January.....October
  February.....November
  March.....December
  April..... January
  May.....February
  June.....March
  July.....April
  August.....May
  September.....June
  October.....July

November.....August
December.....September

National Sex Offender Registry and Known or Suspected Terrorist File records are selected for validation under an alternative procedure. See National Sex Offender Registry File and Known or Suspected Terrorist File chapters for details.

The FBI's CJIS Division policy states that records in the Vehicle, Boat, Gun, Vehicle/Boat Part, License Plate, and Securities Files and qualifying records in the Article File must be validated only once when they are 60-90 days old. However, CSAs must request to participate in the one-time only validation by contacting the FBI CJIS Division at (304) 625-3000.

For all other person files, the first 60-90 day validation should be performed according to the validation rules set forth in the Validation section of this chapter. Subsequent validation cycles require contact with the court or other appropriate source to verify the validity of the record.

- The NCIC System sorts records by CSA. On a monthly basis, the CSAs are advised when a file of records to be validated can be retrieved by way of a $.B. File-Transfer-Ready Notification. Upon receiving this $.B. administrative message, the CSA has 30 days to initiate a file transfer before the file will be deleted. Within the file of records to be validated, each record is presented as a $.C. Request for Validation Notification or in the validation fixed format. The CSA distributes the records to be validated to the ORIs as appropriate. CSAs must certify completed validation to the FBI's CJIS Division prior to the first Sunday of the second month following the date the validation material was made available by the FBI.

  The sequence of records included in the file is as follows:

  - Wanted
  - Gang/Terrorist Member
  - Missing
  - Protection Order
  - Supervised Release
  - Sex Offender
  - Immigration Violator
  - Identity Theft
  - Protective Interest
  - Violent Person
  - Unidentified
  - Boat
  - License Plate
  - Vehicle/Boat Part
  - Vehicle
  - Gun
  - Securities
  - Article

If the record, excluding National Sex Offender Registry records, has been validated electronically within the last calendar month, then the record is considered validated and is not included in the file of records to be validated. If a National Sex Offender Registry record was validated electronically within the last 11 months, then the record is not included in the file of records to be validated.

- Article File records containing a TYP Field codes beginning with "Q" and "T", or "Z" will be validated as described in the Validation schedule above. Other Article File records are not included in the validation process since they have a short retention period. The NICS Denied Transaction File records are also not subject to validation, since these records are a subset of data maintained by the NICS. All other files are subject to validation.
- Each agency must keep in mind the synchronization of records. The records being validated will be chosen by date of entry, Eastern Standard Time (EST) into NCIC. Agencies located in a different time zone must realize that the validation will include records entered after midnight EST on the first of the month through midnight on the last day of the month. The $.C. demonstrates the validation format.

3.4.2 Validation Procedures

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.

3.4.3 Validation Acknowledgment, Certification, and Response

- CSAs are responsible for verifying the receipt of the monthly validation material. If a CSA does not receive the validation material, the CJIS Systems Officer (CSO) or his/her designee must advise the FBI's Data Integrity Staff at <acjis@leo.gov>.
- It is the CSA's discretion as to the method for completing validation.

Validation certification means that:

- The records contained on the validation listing have been reviewed by the originating agencies;
- The records which are no longer current have been removed from NCIC active database and all records remaining in the System are valid and active;
- Records contain all available information; and
- The information contained in each of the records is accurate.
- Certification response conditions:
- The certification response, whether via the Name of Validator (VLN) Field, paper certification, or The International Justice and Public Safety Network (NLETS) message must be returned to FBI CJIS prior to the first Sunday of the second month following the date the validation file was made available by the FBI.

CSAs that choose to certify completed validation via an NLETS message must contact the FBI's Data Integrity Staff at <acjis@leo.gov> prior to implementation. The NLETS message must be transmitted to the FBI at ORI DCFBIWA03 within the designated time frame.

- If a CSA has not received a certification response from an agency under its service jurisdiction in time to certify to FBI CJIS that all records have been validated, the CSA shall remove from NCIC all records, **except** Unidentified Person Records, which are the subject of that agency's validation

listing.

- If a CSA fails to certify any validation listing to the FBI CJIS within the specified time, FBI CJIS shall remove all of that state's/federal agency's invalidated records, except for Unidentified Person File records.

3.5 HIT CONFIRMATION PROCEDURES

- Any agency which receives a record(s) in response to an NCIC inquiry must confirm the hit on any record(s) which appears to have been entered for the person or property inquired upon prior to taking any official actions based upon the hit NCIC record:
  1) arresting the wanted person,
  2) detaining the missing person,
  3) seizing the stolen property,
  4) charging the subject with violating a protection order,
  5) denying the subject the purchase of a firearm, or
  6) denying the subject access to explosives as regulated under the Safe Explosives Act.

  Additionally, an agency detaining an individual on local charges where the individual appears identical to the subject of the wanted person record and is within the geographical area of extradition must confirm the hit.

  Note: The above list is not inclusive of all scenarios.

  Confirming a hit means to contact the agency that entered the record to:

- Ensure that the person or property inquired upon is identical to the person or property identified in the record;
- Ensure that the warrant, missing person report, protection order, or theft report is still outstanding; and
- Obtain a decision regarding:
  1) the extradition of a wanted person when applicable,
  2) information regarding the return of the missing person to the appropriate authorities,
  3) information regarding the return of stolen property to its rightful owner, or
  4) information regarding the terms, conditions, and service of a protection order.

  The above list is not inclusive of all scenarios.

  Note: The source documents used for hit confirmation may be electronic if the local agency has implemented the controls required by the CSA for electronic documents supporting NCIC records.

- Determine if the entering agency wants the record to be located when the missing person was identified by partial body parts.
- Hit confirmation procedure is based on two levels of priority: Urgent and Routine.

Priority 1: Urgent

The hit must be confirmed within 10 minutes. In those instances where the hit is the only basis for detaining a suspect or the nature of a case requires urgent confirmation of a hit, priority 1 should be specified.

Priority 2: Routine

The hit must be confirmed within 1 hour. Generally, this priority will be used when the person is being held on local charges, property has been located under circumstances where immediate action is not necessary, or an urgent confirmation is not required.

- After establishing the priority level, the agency should then follow these procedures:
- Upon receipt of a hit confirmation request, the ORI of the record must furnish a substantive response within the designated timeframe, i.e., a positive or negative confirmation or notice of the specific amount of time necessary to confirm or reject.
- If the agency requesting confirmation does not receive a substantive response within the designated timeframe, the agency should generate a second request with a copy to its CSO and to the CSO of the agency that originated the record. The CSO (or his/her designee) of the originating agency will initiate appropriate action to ensure proper response to a hit confirmation request and to comply with System standards. The CSO action must include canceling the record.
- If the agency still fails to receive a response, the agency should then notify the NCIC Quality Control staff by a third message with a copy to the CSAs involved. Failure on the part of any CSA to ensure such compliance will be brought to the attention of the APB.
- NLETS is the recommended network for hit confirmation. Even if the initial confirmation is handled via telephone, NLETS should be used for documentation. NLETS has created an inquiry (YQ) and a response (YR) format for hit confirmation.

Responsibilities for the hit confirmation process are shared between the agency that received the hit and the agency that enters the record.

- Every agency upon taking a person into custody identifying a missing person, or acquiring property, after confirming the hit, must place a locate on the corresponding NCIC record(s).

Exception: If the missing person has been positively identified by body parts, the locating agency should determine if the entering agency wants the record to be located. The record may remain in NCIC for future positive identification in the event additional body parts are subsequently recovered.

- Agencies using ERMS are encouraged to maintain copies (electronic or hard copy) of hit confirmation information, to include YQ and YR messages, to assist in the event that the agency needs to substantiate the actions(s) it has taken pertaining to a hit confirmation.

3.6 HEADERS

- A header is a sequence of characters acceptable to the NCIC computer which is used to provide message information for the CSA. A header will not be stored as part of any NCIC record (other than the transaction log), but will be held temporarily during processing of the incoming message and returned to the originating terminal as the first item in the NCIC System's response and/or acknowledgment.
- **Header Requirements**:
- Each header must contain a minimum of 9 characters and may contain a maximum of 19 characters.
- All characters must be from the NCIC Character Set as described in the CHARACTER SET

section of this chapter.

- The first 4 characters of the header are used by the NCIC System for appropriate routing.
- Positions 5 through 19 are reserved for the user agency. Characters 18 and 19 are reserved for use by the NCIC workstation in addressing Mobile Imaging Units (MIUs). This is applicable only when the transaction was originated by a MIU developed by the NCIC program or one using the software developed by NCIC.
- **Header Prefixes**:
- 1N01 -- Directs the message to any one of the NCIC files, i.e., all person and property files. The 1N01 header on an incoming transaction indicates the user is performing a transaction using the NCIC format.
- TN01 -- Directs the message to any one of the test NCIC files, i.e., all person and property files. The TN01 header on an incoming transaction indicates the user is performing a test transaction using the NCIC format (except image transactions).
- 1B01 -- Is used when NCIC image transactions are performed, i.e., the following MKEs: Enter Image (EIM) or Modify Image (MII).
- TB01 -- Directs the message to the test NCIC hot files when NCIC test image transactions are performed, i.e., the following MKEs: EIM, and MII.
- 2L01 -- Directs the message to the NGI/III File.
- 6L01 -- Directs the message to NICS.
- ML01 -- Directs the message to NLETS.
- The NCIC response to any transaction begins with a header in which the first 4 characters identify the type of response that follows, i.e., the last transmittable unit of a response contains L in the second position (1L01); each transmittable unit belonging to the same response contains a unique sequence number in position 2 through 4 of the header (e.g., 1011); the second digit of the response header is either L (last transmittable unit) or O; and the next two digits may be anything from 01 to 99.

3.7 CHARACTER SET

- The NCIC character set is comprised of the alpha characters A through Z, the numeric characters 0 through 9, the comma (,), the dollar sign ($), the ampersand (&), the hyphen (-), the blank or space, the slash (/), the asterisk (*), the pound sign (#), the left parenthesis (( ), the right parenthesis ( )), the plus sign (+), the semicolon (;), the percent sign (%), the apostrophe ('), the at sign (@), the tilde (~), the exclamation point (!), the quotation mark ("), the caret (^), the underscore (_), the grave accent (`), the equal sign (=), the opening brace ({), the closing brace (}), the less than sign (<), the greater than sign (>), the question mark (?), the colon (:), the opening bracket ([) , the closing bracket (]) , the reverse slant (\), and the vertical bar (|).

  For NGI/III inquiries, the allowable character set is comprised of the alpha characters A through Z, the numeric characters 0 through 9, the comma (,), the dollar sign ($), the ampersand (&), the hyphen (-), the blank or space, the slash (/), the asterisk (*), the pound sign (#), the left parenthesis ((), the right parenthesis ()), the plus sign (+), the semicolon (;), the percent sign (%), and the apostrophe (').
- A period (.) is used as a delimiter only. It must be used to end each field of data in the message except the last field prior to the end of transmission (EOT) in which case the period is optional.

- The NCIC System automatically changes the alphabetic "O" used in NCIC transactions to the numeric (0). The alphabetic "O" will only appear in the message field codes, ORI records in response to an inquiry, and informational and/or instructional phrases transmitted by the NCIC System. For example: DOB, DCOSI0000, NO NCIC RECORD, and IMMED CONFIRM RECORD WITH ORI. Headers are not converted, even though an O in any of the first 4 positions would be rejected.

3.8 RETENTION OF TERMINAL-PRODUCED PRINTOUT

- When an operational inquiry on an individual or property yields a valid positive response (hit), the terminal-produced printout showing the inquiry message transmitted and the record(s) on file in NCIC should be retained for use in documenting probable cause for the detention of the missing person, arrest of the wanted person, or seizure of the property. The printout may also prove valuable in a civil suit alleging a false arrest, a false imprisonment, a civil rights violation, or an illegal seizure of property. If two-part paper is used, either the original or the legible copy is admissible in federal court. Whether a state court will accept the legible copy or whether only the original will suffice depends on the state's rules of evidence.
- When an NCIC inquiry yields a hit, the terminal employee making the inquiry should note on the terminal-produced printout precisely how, when, and to whom the information was given, initial and date this notation, and forward the printout to the inquiring officer or agency for retention in the case file. This procedure establishes the chain of evidence for the communication should the arresting officer need to substantiate actions in a judicial proceeding.
- The printout should be retained for as long as there remains any possibility that the defendant will challenge the arrest, search, or other law enforcement action taken because of the information contained on the printout. The printout should be retained until all possible levels of appeal are exhausted or the possibility of a civil suit is no longer anticipated.

3.9 NAME MATCHING

- The technique used to match the name in an inquiry with the name in a record on file in NCIC is called the New York State Identification and Intelligence System (NYSIIS). NYSIIS coding is used in the Name (NAM), Alias (AKA), Person with Information Alias (PAK), Person with Information Name (PIN), and Protected Person Name (PPN) Fields of the person files and the Owner (OWN) Field of the Securities File where the owner is an individual. When the inquiry includes both NAM and DOB, primary hits are determined by using a phonetic encoding of the last name and an exact match on the input month, day, and year of birth. An extended NYSIIS algorithm is used.

2. If the input last name corresponds to a name within a list of common surnames, the primary hit is further qualified by comparing the first character of the input given name to the first character of a given name on a person's record.

- If the input given name corresponds to a list of NCIC nicknames, it is replaced by a corresponding proper name specified in the nickname for search purposes. For example, Bill is replaced with William and Betty is replaced with Elizabeth.
- If the input last name contains a hyphen (-), primary hits are determined by using each hyphenated name part as a last name as well as all combinations of the hyphenated name parts. For example, a surname of Saenz-Parada-Lopez will be searched as Saenz-Parada-Lopez, Saenz-Lopez-Parada, Lopez-Parada-Saenz, Lopez-Saenz-Parada, Parada-Lopez-Saenz, Parada-Saenz-Lopez, Saenz, Parada, and Lopez.
- **Expanded Name Search**: If the input value of ENS is the character "Y" and NAM and DOB are

specified, primary hits are determined using each input name part as a last name, interchanging the remaining name parts as given names. For example, Bryan, Morgan Lee; Bryan, Lee Morgan; Morgan, Lee Bryan; Morgan, Bryan Lee; Lee, Morgan Bryan; and Lee, Bryan Morgan.

- **Expanded Date of Birth Search**: If the input value of the EBS Field is the numeric 1, primary hits are determined by NCIC searching the exact month and day and a range of plus or minus 1 year of the input date of birth.

  If the input value of the EBS Field is the numeric 2, primary hits are determined by an NCIC search of records with the exact year and month and day of the input date of birth transposed.

  If the input value of the EBS Field is the numeric 3, primary hits are determined by an NCIC search of records with the exact month and day, plus or minus 1 year, and records with the month and day of the input date of birth transposed.

  If the EBS Field is not included or is blank, primary hits are determined by an NCIC search of records with the exact date of birth.

3.10 NAME SEARCH IN NGI/III

The NGI/III name search technique is explained in detail in the NGI/III chapter.

3.11 TERMINAL AND/OR LINE FAILURE

- Every effort will be made to notify users on-line when the NCIC computer is going out of service. However, when NCIC goes out of service unexpectedly, an out-of-service message cannot be sent. Operational failure of a user's terminal may result from one of four conditions:
- The NCIC computer is out of service;
- The control terminal fails or is out of service;
- A circuit problem; or
- The user's terminal malfunctions.

A CSA should make every effort to verify that the difficulty does not lie within its terminal equipment. If the difficulty is a terminal malfunction, the CSA should notify the local terminal maintenance office for repair.

- System activity and line traffic are monitored at the NCIC computer center. When there is line difficulty or malfunctioning of a data set, the area office of the vendor providing communication service is immediately notified by FBI CJIS. It is not always possible to make a specific diagnosis of the trouble at the FBI CJIS. In some cases, it is only known that an agency is not responding or is not responding properly to the NCIC computer. If, after a reasonable amount of time, the user's problem has not been rectified, FBI CJIS will notify the appropriate vendor.
- When an out-of-service status and an analysis indicate that the problem is not terminal equipment difficulty such as power supply, paper supply, switches improperly set, or terminal malfunction, a CSA should:
- Immediately notify the local vendor providing communication service;
- Log the time of notification;
- Note the circumstances relating to the problem; and
- If after a reasonable period of time the vendor's efforts have not resolved the problem, notify the

FBI CJIS (telephone 304-625-HELP [4357]) of the time the vendor was notified and a brief description of the problem.

3.12 FILE REORGANIZATION AND PURGE SCHEDULE

During the monthly purge cycle, NCIC sends the $.P. notifications to the ORIs informing them their record has been retired. The System will no longer require restricted service during the monthly purge process. NCIC retires records immediately at the end of their retention period, making them accessible only through an SPRQ search.

3.13 NGI/III FILE RESTRICTED SERVICE

Users are advised of restricted service periods through on-line transmissions of NCIC administrative messages. When the NCIC System goes out of service for more than 15 minutes without NCIC having previously sent an out-of-service message, a NLETS All Points Broadcast is sent to advise users of the outage.

3.14 NCIC NUMBERS (NIC NUMBERS)

Each record entry message that is accepted for storage in the NCIC System is assigned a unique **NCIC Number (NIC)** for record identification purposes.

- If the prefix of the NIC is a single alphabetic character, the NIC has 10 characters, consisting of an alphabetic character that identifies the NCIC file in which the record is indexed, a 7-character unique number, and 2 check digits.
- If the prefix of the NIC is double alphabetic characters, the NIC has 10 characters, consisting of double alphabetic characters that identify the NCIC file in which the record is indexed, a 6-character unique number, and 2 check digits.

  The first character of the File Indicator will remain static, and the second alphabetic character will indicate the NCIC file. The first alphabetic character will be designated as a "Y." The "Y" will indicate that the second alphabetic character must be used to determine the NCIC file in which the record is indexed. The second position may be any alphabetic character (except O).
- The 2 check digits are used to validate NICs when they are used in inquiry messages and when they are used to identify records in modify, locate, cancel, and clear transactions.

3.14.1 NIC Check Digit Algorithm

When an NIC is used as an identifier in a cancel, clear, inquiry, locate, or modify message, the NCIC verifies the validity of the number using the two check digits, i.e., the last two characters of the number. The following algorithms are used for the process:

If the prefix of the NIC is a single alpha character, the digits of the sequential number (positions 2 through 8 of the number) are multiplied by a value, as follows:

	Multiplication Factor
Position 2	8
Position 3	7
Position 4	6
Position 5	5
Position 6	4