KINGMAN COUNTY SHERIFF'S OFFICE
POLICY AND PROCEDURES MANUAL
AUTHORITY: SHERIFF RANDY L. HILL
EFFECTIVE DATE: July 1, 2016
Number of Pages 35

SECTION 5.2
NCIC – CJIS – KCJIS
STATE OF KANSAS

AUDIT STANDARDS FOR THE PRIVACY AND SECURITY OF KCJIS-SENSITIVE INFORMATION

The Kingman County Sheriff's Office has adopted the following: Audit standards that are based on the KCJIS Policy and Procedure Manual, FBI CJIS Security Policy, Title 28, NCIC Operating Manual, Federal and State statutes and other applicable sources.

Part One - NCIC System Quality Assurance

All NCIC entries must be timely, accurate and complete.

Section A: NCIC Entry Procedures

1. Timely Entry

Timeliness requires that records are entered immediately when the conditions for entry are met, not to exceed 72 hours, upon receipt by the entering agency of the source document(s) supporting the entry. This can be documented by "time and date stamping" the report (i.e.; theft, missing person, etc.) when received from the case officer or the warrant, protection, stalking or restraining order when received from the court.

NCIC deviates from the 72 hour limit for timely entry when an agency takes a missing juvenile report. In such cases the entry should be made immediately, as soon as the minimally required information is available to make an entry, not to exceed 2 hours.

The State of Kansas requires, per KSA 75-712c, that ALL missing persons, regardless of age, be entered in NCIC immediately, as soon as the minimum information is available to make an entry, not to exceed 2 hours.

The only exception to immediate entry are when otherwise prescribed by Federal law or when documentation exists to support delayed entry.

The only exceptions to immediate entry are when otherwise prescribed by Federal law or when documentation exists to support delayed entry.

NCIC records shall also be modified, cleared, and canceled promptly to ensure maximum system effectiveness and as an effort to limit potential liabilities upon the entering agency.

2. Packing the Record

Complete records of any kind 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:

(a) Increase the likelihood of a positive hit on the subject or property and aid in the identification of a subject or property

...or...

(b) Assist in compliance with applicable laws and requirements

Criminal History Record Information (CHRI) inquiries must be made at all applicable federal, state and local levels. This would include a III inquiry and a check via any City, County and/or State where the subject is known to have resided and/or worked. Kansas, and other states, Computerized Criminal History (CCH) records are potential sources of information which may contain identifiers not found in a NCIC III record.

A positive response to these inquiries may reveal not only physical descriptors, identifying numbers and aliases not previously known to the inquiring party but also arrest, court, custody and/or supervision data which might provide investigative leads.

A DMV inquiry, i.e.; driver's license data for person entries and registration data for vehicle entries, must be made on all qualifying entries to obtain additional data to add to the entry. Copies of any DMV records utilized to support the entry shall be kept in the case file for documentation purposes.

Although not indicated as a minimally required field in the entry form(s), if citizenship information is available, typically via the CHRI, the Citizenship Field must be completed. If multiple citizenship information is found, a supplemental entry must be completed to include all citizenship data in the entry.

Any supplemental data received after the original entry must also be documented in the case file.

3. Entry Worksheet

An entry worksheet must be completed and retained in the case file for every NCIC entry.

4. Second Party Checks

The accuracy of NCIC records shall be double checked by a second party. This verification shall be completed by someone other than the person making the entry. The individual conducting the second party check need not be NCIC certified. The second party check shall ensure all available cross checks were made and that the data entered matches the supporting documentation. The completion of the second party check must be documented on the entry worksheet.

5. Supporting Documentation

Documentation supporting data entered in each field of an NCIC entry shall be maintained in the case file. This would include, but is not limited to, KSOR's, court orders, investigative reports and NCIC entry worksheets. When supplemental data is received, such as a serial number, VIN number, or personal identifying information from DMV, the documentation for that supplemental information shall be placed in the case file.

Copies of III, or other forms of CHRI, may be retained in the case file at the Sheriff's discretion.

The supporting documentation for active NCIC entries shall be easily accessible and not stored in remote areas of the department or buildings outside the agency. All case files supporting NCIC entries shall be placed in a centrally located active file that is easily accessible to records and/or dispatch personnel. This will allow for easier validation of records and confirmation of hits on your entries.

Agencies that have converted to a paperless records system will not be required to create a paper file on any transactions conducted on these entries for audit purposes. The auditor will prearrange with the agency a mutually agreeable method of gaining access to the case files selected for review in the audit process.

6. Use of the Served Agency's ORI

If an agency makes an NCIC record entry for another agency, the ORI Field of the record shall contain the ORI of the served agency.

If, however, the agencies enter into a Holder of Record agreement via which the served agency agrees to furnish a copy of all supporting documentation to the serving agency for hit confirmation purposes, the entry may be made under the ORI of the serving agency.

Section B: NCIC Entry Procedures Specific to the Files Audited

WANTED PERSON

1. Wanted Person entries are based on a valid warrant

The criteria for entry is any individual, including juveniles, for whom a federal, a felony or misdemeanor warrant is outstanding may be entered into NCIC. Probation and parole violators meeting the criteria described above may also be entered in to NCIC.

2. Entries may be made on felony and misdemeanor warrants (extraditable or non-extraditable). Extradition is authorized before entry is made in the file, if applicable

Before entering a record of a wanted person in NCIC, the entering agency shall attempt to determine to the maximum extent possible, if extradition will be authorized if the individual is located in another state.

At the time of entry, if there is a limitation concerning extradition of the wanted person, such information shall be entered using the appropriate code in the Extradition Limitation (EXL) Field with any specific limitations placed in the MIS Field of the record.

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 (NOEX) in the Extradition Limitations (EXL) Field.

For felony records the extradition (EXL) Field Codes are:

(1) Full Extradition, unless otherwise stated in the MIS field
(2) Limited Extradition - See MIS Field (requires limitations listed in the MIS Field)
(3) Extradition - Surrounding States Only
(4) No Extradition
(5) Extradition Arrangements Pending - See MIS Field (requires explanation in the MIS Field)
(6) Pending Extradition Determination - See MIS Field (requires explanation in the MIS Field)

For misdemeanor records the Extradition (EXL) Field Codes are:

(A) Full Extradition

(B) Limited Extradition - See MIS Field (requires limitations listed in the MIS Field)
(C) Extradition - Surrounding States Only
(D) No Extradition
(E) Extradition Arrangements Pending - See MIS Field (requires explanation in the MIS Field)
(F) Pending Exradition Determination – See MIS Field (requires explanation in the MIS field)

If you do not enter any information in the EXTRADITION LIMITATION (EXL) FIELD, the field automatically defaults to FULL EXTRADITION.

PROTECTION ORDER

1. **Reasonable attempt to serve before entering a Protection order**

   Before entering a Protection Order record into NCIC, there must be a reasonable attempt made to serve the order upon the subject against whom the order is issued.

   In an event an order is not served prior to entry, a notation to this effect must be included in the Miscellaneous (MIS) Field.

2. **Date of expiration (EXP) of the Protection Order**

   The expiration date is the date the order expires. If the order does not have an expiration date**, NONEXP** shall be entered.

3. **Protection order conditions (PCO)**

   The terms and conditions of the order are indicated in the PCO Field. An additional eight conditions may be added by entering a supplemental record. PCO codes are listed in the entry section of the Protection Order File of the NCIC Operations Manual.

4. **Exclusive rights to the residence**

   If a protection order grants exclusive rights to, or sole possession of, the property or residence to either party, the specific address of the residence shall be entered in the Miscellaneous Field.

5. **Specify the type of order in the Miscellaneous (MIS) Field**

   The type of protection order must be clearly indicated in the miscellaneous Field…i.e.; "Protection from Abuse", "Protection from Stalking", "Restraining Order", etc.

6. **Brady Indicator and Protection Order Condition (PCO) Code 07**

The Protection Order File allows for two immediate indicators to identify whether a subject is prohibited from the receipt or possession of a firearm, the Brady Indicator (BRD) Field…to be utilized when the subject is prohibited under Federal Law 18, USC 922 and the Protection Order Condition (PCO) code 07…which should be applied when the subject is state prohibited.

Only final Protection Orders may contain a Brady indicator of Y (yes) or U (unknown). If the subject is not Brady disqualified N (no) must be used.

The Protection Order File section of the NCIC Manual contains a chart of relationships frequently encountered on protection orders and the appropriate determination for the application of the Brady indicator in the NCIC entry.

Judges may apply any reasonable restrictions upon the subject of a protection order which are deemed to be appropriate for ensuring the safety of the protected person(s). The PCO 07 provision is indicated when the court checks the box under "Other Provisions" on the court order form indicating "Defendant shall surrender any firearms to..." and/or includes wording to this effect in the order. This condition code may be applied regardless of any federal prohibition and does not require the same "intimate partner" relationship as the Brady Indicator.

When an agency enters a POF record with a protection order condition of "07" and a weapon other than a firearm is specified, the weapon must be identified in the MIS Field.

7. **Protected person name (PPN) and supplemental for additional protected persons**

Although not a minimally required field for entry per NCIC, if the name of the primary protected person is known, and the use of the name is not otherwise restricted due to safety or privacy concerns, the name must be placed in the PPN Field in order to be "searchable" data for triggering a hit.

If there are additional protected persons named in the order, including children, these should be added in a supplemental entry. If a name is hyphenated the hyphen must be placed between the surnames.

MISSING PERSON

1. **A missing person report is required to make an entry in the Missing Persons file**

A missing person record may be entered under the category of (a) disability, (b) endangered, (c) involuntary, (d) juvenile, (e) catastrophe victim or (f) other. Only the

agency holding the missing person report may make, or cause an NCIC entry to be made.

2. The signature of a reporting party is required before entering an emancipated missing person

A record for a missing person who is declared emancipated as defined by the laws of his/her state of residence (18 years of age in Kansas) may be entered in the Missing Person File provided the entering agency has signed documentation in its possession supporting the stated conditions under which the person is declared missing. This written documentation will aid in the protection of the individual's right to privacy.

In the absence of documentation from a parent, legal guardian, next of kin, physician or other authoritative source including friend or neighbor in unusual circumstances, a signed report from the investigating officer may suffice. The officer signing under these circumstances assumes any potential liability which might arise from an inaccurate report.

3. Missing juveniles under the age of 13

The Kansas message switch has been programmed to restrict users from entering children under the age of 13 as simply a missing juvenile (EMJ). The message switch will reject any such attempt and direct the agency to enter the missing juvenile as "missing endangered" (EME or EMEC) or "missing involuntary" (EMI or EMIC).

VEHICLE

1. Criteria for entry

A vehicle is defined as any motor driven conveyance designed to carry its operator except a boat. Included are aircrafts and trailers.

A stolen vehicle may be entered if a theft report has been made. A loaned, rented or leased vehicle that has not been returned may be entered if an official police theft report is made or a complaint results in the issuance of a warrant.

A felony vehicle may be entered immediately providing the whereabouts of the vehicle is unknown.

A vehicle subject to seizure may be entered when based upon a federally issued court order.

2. Proper entry Message Key (MKE)

The entry MKE of "EV" is used for the majority of Vehicle File entries and is translated to be "Stolen Vehicle".

If the vehicle is being entered as a "Felony Vehicle" (not stolen but reasonably believed to have been used in/during the commission of a felony) the appropriate entry MKE is "EF".

3. Caution indicators

When appropriate, caution indicators must be included in the entry and the following will be appended to the MKE...

- **A Occupant is armed**
- **P Hold for latent prints**
- **F Occupant armed and hold for prints**

4. Source Documentation

Source documentation for VIN's shall be obtained and retained in the case file. Documentation may include certificates of title or origin, registration receipts, DMV printouts, bills of sale and insurance documents.
Your agency shall also check VIN's for passenger vehicles, trucks, buses, trailers, motorcycles, ATV's and incomplete vehicles manufactured after 1981 to ensure they meet the 17 character VIN requirements.

The OAN field for a vehicle entry shall be properly utilized for non-conforming or state assigned VIN's. Vehicles that have a second identifying number (such as an engine number) should be entered by placing the VIN in the VIN field and the additional identifying number in the OAN field.

IDENTITY THEFT

1. Incident report required for entry in the Identity Theft File

When a victim becomes aware that his/her identity has been stolen and reports the incident to law enforcement, the officer shall complete an incident report and collect pertinent information from the victim to create a victim profile.

2. Consent waiver

Information is entered into NCIC only after the victim signs a consent waiver. This waiver shall state that the victim provides permission for the information to be entered in the Identity Theft File. The waiver shall also include the victim's permission to use their SOC as part of the entry.

The waiver also acknowledges that the victim may withdraw his/her consent to the entry in NCIC by providing a written notice to the entering agency.

3. Password

The victim shall select a password when the police report is filed. The password may be eight to twenty alphabetic, numeric or special characters. The password must be included in the entry.

NATIONAL SEX OFFENDER REGISTRY (NSOR)

1. Criteria for entry

Any Sex Offender required to register under the Kansas sex offender registry program has met the NCIC criteria for entry.

2. Noncompliant offenders

The agency may enter in the NSOR records for offenders who have failed to register or are noncompliant with an explanation (i.e.; absconder) in the Miscellaneous Field.

3. Modifications of NSOR records

Any modification of information in the NSOR is to be completed as soon as possible, not to exceed 3 days, upon the agency's receipt of the information supporting the modification.

Section C: NCIC Validation Procedures

Validation requires the agency holding the case file to confirm the record is complete, accurate and still outstanding or active. Validation is accomplished by reviewing the original entry and current supporting documents, and by recent consultation with the appropriate prosecutor, court, or other appropriate source or individual. The validation process includes a review of whether additional information has become available that could be added to the entry being validated.

1. Wanted Person and Protection Order entries

The court and/or prosecutor are contacted to determine if the protection from abuse/stalking/restraining order or the warrant supporting a wanted person entry is still outstanding and extradition (if applicable) is still authorized.

2. Vehicle, Missing Person and Identity Theft

For stolen property, missing person and/or Identity Theft File entries the reporting party is to be contacted to determine if the case is still active and the continued maintenance of the NCIC entry is appropriate.

In the event the agency is unable to make contact with the complainant or reporting party, the agency shall make a determination based on the best information and knowledge available, whether or not to retain the original entry in NCIC. The

determination by the agency to retain an entry in NCIC when contact with the party responsible for reporting the subject or property is unsuccessful means the agency is assuming liability for the entry.

3. National Sex Offender Registry

As the offender is required to register repeatedly throughout the year, and the registering/entering agency is expected to update the associated NCIC NSOR record entry as appropriate at each registration, the Validator's Name (VLN) and Validation Date (VLD) can be modified at the same time. This process will keep the NSOR entry continuously validated.

If an offender has moved to another state which does not require registration, the Kansas agency is to leave their entry in NCIC. Change the State (STA) Field to reflect the appropriate state and add to the MIS Field a statement clearly describing the current circumstances.

If an offender has been deported or moved/traveled internationally, the entry should be maintained in NCIC and the NCIC assigned country code, as listed in the NCIC Code Manual, should be entered in the STA Field.

The validation of the records for those individuals who are not available to appear for registration will then be required on an annual basis. The process in these cases will consist of little more than confirming with the Offender Registry Unit of the Kansas Bureau of Investigation that the individual is still actively listed on the Kansas registry and would be required to resume registration upon returning to Kansas.

4. Supporting files and documentation are reviewed to determine there is a source document on which the entry is based

The case file and documentation supporting an NCIC entry shall be reviewed in the validation process. The NCIC entry worksheet is not sufficient for validating an entry because it may contain inaccuracies. Every field of information on the worksheet originated from some other source and it is that source that shall be used to validate the record.

The printouts or field notes supporting information entered in fields of an NCIC entry shall be stored in the case file and reviewed during validation. The information shall be compared against the data in the entry to determine its accuracy.

III and state criminal history record inquiries shall be made to determine if new identifiers have become available since the last validation. If there is new, or different, information available, the record shall be modified and/or supplemented during the validation process.

5. Validation worksheet

A validation worksheet must be completed to document the steps taken/contacts made in the validation process. The worksheet associated with the most recently completed validation process shall be retained in the case file.

Section D: NCIC Hit Confirmation Procedures

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

a. Ensure that the person or property inquired upon is identical to the person or property identified in the record.
b. Ensure that the warrant, missing person report, protection order, or theft report is still outstanding and
c. 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 and conditions of a protection order

2. Nlets YQ and YR formatted messages are used to confirm NCIC hits

In order to standardize the hit confirmation transaction, a fixed format hit confirmation is used. This message is sent via Nlets utilizing a unique message type for inquiry (YQ) and response (YR). When requesting confirmation on a hit or responding to a request for confirmation, it is imperative that agencies use the "YQ" and "YR" respectively.

3. Response to urgent priority hit confirmation request is made within ten minutes

Utilize "U" for Urgent in the PRI/field when requesting a response within ten minutes. Urgent requests are to be used when the hit is the only basis for detaining a suspect or the nature of the case requires urgent confirmation of a hit.

4. Response to routine priority hit confirmation request is made within one hour

Utilize "R" for Routine in the PRI/field when requesting a response within one hour. Routine requests are to be used when the person or property is being held on local charges or when an urgent confirmation is not required. Agencies are encouraged to use the lower priority when an immediate response is not necessary.

5. Wanted person detainer

A detainer is an official notice from a government agency to a correctional (incarcerating) agency requesting that an individual wanted by the first agency, but subject to the correctional (incarcerating) agency's jurisdiction, not be released or discharged without first notifying the wanting agency and giving them an opportunity to respond. Typical reasons for a detainer include the individual is wanted for trial or wanted to serve a sentence in the requesting jurisdiction.

Only Wanted Person File records in located status may receive detainer information. When an inquiring agency receives a positive response, confirms the warrant is outstanding and authorizes extradition, that agency must perform a locate transaction to place the record in located status. If the locating agency intends to hold the individual on local charges, the locate transaction should indicate detention by placing DETN (detention) in the Extradition (EXT) Field.

Located records which contain EXTR or DETN in the EXT Field remain online for five days. The wanting agency is notified of the locate by way of the $.L. (locate notification) administrative message. The wanting agency can ascertain the intent of the locating agency via the contents of the EXT Field or through direct communication with the locating agency. At that point, the record may have a detainer appended by the wanting agency. A Wanted Person record will remain active in NCIC as long as the detainer is appended. Five days prior to the date of sentence expiration, the wanting agency is notified of the impending release.

Permitting a Wanted Person record to remain active in NCIC while the subject is being held in another jurisdiction enables the detainer to be identified and the subject to be extradited rather than released. The detainer capability does not alter the need for correctional and/or jail facilities to query NCIC to determine if warrants exist prior to an individual's release

.

Section E: Removal of NCIC records

1. A clear message is used to remove a record from NCIC when the subject of an entry has been located

A clear message is used when the apprehending or recovering agency is the agency that entered the record, or when notified that the subject of the entry is in the custody of another agency (does not apply when the wanted person record is in a detainer status), or the object of an entry has been recovered.

2. A cancel message is used to remove an NCIC record that is no longer valid

A cancellation message is utilized when the entering agency determines that the record is invalid. This could be as the result of a warrant being dismissed or recalled, when a missing person returns home of their own accord, or the entering agency making the determination that a false report has been filed.

3. **Inquiry by NIC following removal**

After removing an NCIC record (clear or cancel), the agency shall run an inquiry by NIC number to ensure the record has been successfully removed and retain the printout of the "NO NCIC WANT" response in the case file.

4. **Identity Theft File record removal**

Records are removed from the Identity Theft File of NCIC by means of a cancellation only.

5. **Retention of the case file**

The supporting case file must be retained until all possible levels of appeal are exhausted or any possibility of a civil suit is no longer anticipated.

Part Two - Security

Section A: Facility Security

(SEE SECTION 5.1, PAGE 9 FACILITY SECUITY PROCEDURES.)

1. **Area is physically secured at all times**

The computer site, terminal area and/or any area where KCJIS-sensitive information is accessed or stored shall have adequate physical security to protect against any unauthorized access. Use of locking files and providing keys or combinations to authorized persons is advised.

2. **Visitors escorted at all times or backgrounded with a name based record check**

Visitors to areas where CHRI is stored and/or a KCJIS terminal resides shall be either escorted at all times or be checked for criminal history with a name-based record check via III, Kansas and/or other state(s) CCH using purpose code "C".

3. **Record storage and disposal**

Copies of the data received from the system printer shall be afforded security to prevent any unauthorized access to or use of the data. KCJIS printouts shall be

protected from accidental observation and inadvertent disclosure when in active use. These printouts shall not be left in open view while unauthorized persons are present. KCJIS printouts shall be transported and maintained under cover. Printouts no longer of use shall be destroyed via shredding, incineration or any means of erasing identifying information so that identities of record subjects cannot be established. Electronic copies shall be erased, destroyed or degaussed by a program specifically for that purpose. Access devices that have had KCJISsensitive information on them shall have any non-volatile memory components removed or destroyed.

4. Lost or stolen KCJIS equipment

Lost or stolen KCJIS-related equipment, including the SecurID tokens, shall be reported to the KBI Help Desk immediately so that access through such equipment can immediately be revoked.

Section B: Personnel Screening
(SEE SECTION 5.1, PAGE 6 PERSONNEL SCREENING.)

1. Appropriate background investigations shall be conducted

All criminal justice applicants and employees who will have authorized KCJIS terminal use access, access to KCJIS-sensitive information or have unescorted access into terminal or network areas shall be a U.S. Citizen or a non-U.S. citizen legally able to perform the work in or for the United States, at least 18 years of age and screened for a record of criminal activity and criminal history as defined in the KCJIS Policy and Procedure Manual prior to employment.

Your agency's security policy shall include a requirement for pre-employment background investigations requiring checks through III and state criminal history files for all employees.

Background investigation records shall be kept separately from the agency's criminal investigation records.

The employment background screening shall minimally include:

Local name based check for criminal history record information.
A query of all states' criminal histories databases via the Nlets "IQ" and, if needed, "FQ" query transactions.
Federal (III) name based check for criminal history record information prior to employment or access to CJI is granted.
Fingerprint submission (within 30 days of employment or assignment) to the KBI who will then forward the fingerprints to the FBI.
A name based query upon Interpol utilizing the Nlets "IPQ" and, if needed, "FPQ" query transactions.
Local and Federal warrant (Kansas Warrant File and NCIC Wanted Person) check.

a. Employees with authorized KCJIS access

When a final applicant or current employee is considered for any position that includes authorized access to KCJIS-sensitive information, a thorough background investigation shall be conducted, to include a fingerprint check in addition to the name based check, as required by the KCJIS Policy and Procedure Manual.

Information Technology (IT) contract personnel are to be backgrounded to the same extent as a criminal justice agency employee due to the nature of the work performed by, and the level of access granted to, these individuals.

b. Employees not authorized KCJIS access

Employees who may inadvertently be exposed to KCJIS-sensitive information in the performance of their duties but cannot obtain it themselves or have the authority to request a terminal operator to obtain specific information on their behalf, shall be screened for a record of criminal activity and criminal history using a name based check as required by the KCJIS Policy and Procedure Manual.

c. Other individuals who may be exposed to KCJIS-sensitive information

Persons who are allowed to perform duties on behalf of a criminal justice agency in such a manner that may expose them to KCJIS-sensitive information in the course of their duties, to include reserves, interns, volunteers, consultants, vendors, contractors (other than the IT contractors), etc., shall be screened for a record of criminal activity and criminal history using a name based check as required by the KCJIS Policy and Procedure Manual.

2. Applicant Fingerprint Card

One Applicant Fingerprint Card is submitted to the KBI for all persons having access to KCJIS sensitive information to determine the existence of any criminal history record.

A fingerprint-based record check must then be conducted within 30 days after initial employment or assignment for those who have authorized KCJIS access or will have unescorted access to KCJIS computer terminal areas or will have unsupervised access for the purpose of maintaining computer software, hardware or computer networks.

Applicant fingerprint cards shall be kept separately from the agency's criminal investigation records.

3. Annual Screening

Although pre-employment background investigations are conducted for all employees and other individuals having access to KCJIS-sensitive information and secured equipment, annual re-checks shall also be performed. The annual screening shall include the same name based checks required at the time of employment...III, Nlets "IQ" query for all states' criminal histories and the Interpol query via the "IPQ"

transaction. Additionally, it is recommended any annual re-screening should include a driver's license check.

Individuals shall also be re-screened at any time the agency suspects the individual may have committed a potentially disqualifying act.

The agency shall prohibit any employee from accessing or reviewing his or her own CHRI.

The following elements are, at minimum, required to be incorporated in the agency's standard operating procedures.

1. Procedures for conducting background investigations

A criminal justice agency is required to screen for employment, all personnel authorized access to KCJIS-sensitive information (Title 28). Your agency security policy shall include preemployment background investigations requiring checks through III and state criminal history files (all states via Nlets IQ/FQ), the Interpol IPQ query, fingerprint based checks and state and national warrant checks for all personnel who will have authorized KCJIS access, or will have unescorted access to a KCJIS computer terminal area, or will have unsupervised access into computer software, hardware, or computer networks.

2. Self-Reporting of any new criminal violation
(SEE SECTION 5.1, PAGE 15 Self-Reporting of any new criminal violation)

An agency must adopt a policy requiring any individual with authority to access KCJIS information to report to the agency head any new indictment, arrest, charge, conviction, or diversion of a criminal violation by the end of the business day following the reportable event.

3. Facility Security Procedures

Each criminal justice agency shall adopt operational procedures reasonably designed to ensure the physical security of the computer site, terminal area and/or where KCJISsensitive information is accessed or stored to protect against any unauthorized access. While each agency is free to develop its own physical security procedures, the procedures shall include:

a. The establishment of physical barriers, sign-in procedures, guards or the use of keys, badges or technological locking devices.

b. The segregation of terminals, files and other physical locations where information is used and displayed so that visual surveillance or eavesdropping is prevented.

c. Written procedures for escorting persons not normally authorized to enter the secured area. All persons must be escorted at all times unless a complete background screening has been conducted per KCJIS Policy.

4. Dissemination guidelines for criminal history record information

A basic review of agency dissemination guidelines shall be stated in the agency S.O.P. Those instances when dissemination of III information is allowed or prohibited shall be specifically addressed. A sanction shall be imposed for inappropriate dissemination per KCJIS Policy and Procedure Manual.

5. III/CHRI access by Mobile Data Computers

Mobile data computers may query and receive detailed III/CHRI information, if allowed by the local agency's policies. A record of criminal history on file may be transmitted to a mobile data computer. (Kingman County Sheriff does not currently use MDT's.)

6. Procedures for accommodating Individual Access & Review of one's own criminal history record

(SEE SECTION 5.1, PAGE 13 Individual Access and Review of One's Own Criminal History.)

All individuals have the right to review and challenge their criminal history record information. However, a local agency is prohibited from providing KCJIS CHRI to an individual or the general public. The local agency shall instruct the individual to contact the KBI for Kansas Criminal History Record Information and/or the FBI or other state that holds the record for III information.

The basis for implementation of Individual Access & Review is contained in K.S.A.22-4704, K.S.A. 22-4709, K.A.R. 10-13-1 and K.A.R. 10-13-2. These procedures should be simply described in an easy to follow format in the agency's S.O.P. so that compliance with the statutes is easily understood and imposes no burden on either the agency or the person exercising this right.

7.Agency specific NCIC system quality assurance

The S.O.P. shall include the agency's requirements and procedures for entry, maintenance, removal and validations of NCIC records. Agency specific checklists

may be incorporated into the procedures. Reliance on NCIC manuals may be included on a secondary basis. An NCIC compliance requirement of complete and accurate entries implies that an agency shall place specific emphasis on the required documentation, proofing of entries and validation procedures.

8. Reporting of violations of KCJIS Policy and Procedure Manual and Security Incidents

When a violation of KCJIS Policy and Procedure occurs at the local level, the local agency administration shall initiate an investigation to determine why the violation occurred, administer appropriate discipline, notify the appropriate KHP CJIS Unit Auditor and submit a report to the CJIS System Officer (CSO) documenting the violation and disciplinary or corrective measures that have been taken. If it is discovered a policy violation occurred at a local agency and the above process was not followed the CSO will open an investigation into the matter.

Incidents that threaten the operation or integrity of the KCJIS system or KCJIS-sensitive information shall be reported immediately to the Local Agency Security Officer (LASO), other agency supervisory personnel, KCJIS Information Security Officer (ISO), and the KBI Help Desk. Steps shall be taken to identify, contain, isolate and document the incident as quickly as possible.

9. Agency will have the right to transfer or remove personnel for violations of local or KCJIS policies

A criminal justice agency shall have the authority to make sure that proper discipline is applied if personnel who have been screened subsequently violate security rules. Title 28 states: "*that a criminal justice agency will have the right to initiate or cause to be initiated administrative action leading to the transfer or removal of personnel authorized to have direct access to such information where such personnel violate the provisions of these regulations or other security requirements established for the collection, storage or dissemination of criminal history record information".*

10. KCJIS access for terminated, resigned or suspended employees

Upon termination, resignation or suspension of an employee the KBI will be notified of the status of the former employee. The former employee must return his/her token to Sheriff or the Communication Supervisor. The Communication Supervisor will immediately contact the KBI Helpdesk to deactivate the token and remove the former employee security clearances from the KCJIS system, as well as, all other criminal justice systems in our department.

11. Agency Internet Use Policy

(See Section 26.0 Use of Internet Policy)

Agency Policy governing e-mailing of KCJIS-sensitive data

The Kingman County Sheriff's Office permits KCJIS-sensitive information (audio and data) to be transmitted by e-mail only when both the sending and receiving e-mail boxes belong to one of the approved domains outlined by the state. Kingman County Sheriff's Office Records staff has secure LEO e-mail addresses for such purposes.

Any employee sending KCJIS sensitive information via e-mail not on an approved secure domain is in violation of this policy. They will be subject to corrective action, including possible termination of employment, legal action, and criminal liability.

Electronic transmission including E-Mail

Level 4 KCJIS-sensitive information shall not be transmitted electronically including e-mail except for the following:

Specific KCJIS information may be transmitted in an unencrypted format to any authorized user. Such dissemination applies to the following types of information:

- National Weather Service Information or KHP Road Reports
- Kansas Humanitarian "attempts to locate", except when it is intended for law enforcement use only.
- Driver's license or other photos provided no personal identifying information (PII) accompanies the photo. Examples of PII include but are not limited to: Driver's license number, FBI number, KBI number, Name or Social Security Number.
-

KCJIS-sensitive information (audio and data) may be transmitted through an approved mobile data computer network meeting minimum encryption requirements, as outlined in the KCJIS Policy and Procedure Manual) to a mobile data access device having a KCJIS-assigned mnemonic.

KCJIS-sensitive information (audio and data) may be transmitted by e-mail only when both the sending and receiving e-mail boxes belong to one of the approved encrypted domains:

leo.gov
mocic.riss.net
rocic.riss.net
wsin.riss.net
adg.riss.net
leiu.org
epicmail.riss.net
magloclen.riss.net
nespin.riss.net
rmin.riss.net
risstech.riss.net
cbi.org
hidta.net

Text messaging is prohibited

KCJIS –sensitive information, with the exception of criminal history record information and intelligence information may be transmitted in audio format unencrypted to any authorized user.

12. Mobile Data Computer usage and physical security

Each agency shall develop and implement written policies and procedures governing the usage and physical security of the mobile data computer terminals, if applicable. (Kingman County Sheriff does not currently use MDT's.)

14. Agency has a written program to train all persons having access to KCJIS

(SEE SECTION 5.1, PAGE 3 TRAINING.)

Within six months of election, selection or assignment all personnel with authorized KCJIS access shall be trained on privacy and security issues regarding KCJIS-sensitive information.

Criminal justice agencies shall adopt CHRI training programs. *"Each employee working with or having access to criminal history record information shall be made familiar with the substance and intent of these regulations"* (Title 28). Inadequate training in privacy, security, completeness and accuracy of criminal history record information, by an administrator of those who shall access the information, may result in the finding by a court that breach of a specific duty has occurred and the persons involved are liable for damages under the general principles of tort law.

The S.O.P. shall contain an organized training program that will include relevant federal, state and agency rules and regulations regarding the access, physical security and dissemination of criminal history records and systems quality assurance.

All employees with access to CHRI records and KCJIS equipment shall be required to read all relevant security rules and instructions and sign or initial the material indicating that they have read and understand them.

Section D: Personnel Training

1. KCJIS training the agency provides is documented

In order to verify that an employee has been trained in specific areas, it is required that some system of documentation of the training conducted be incorporated into the agency training and personnel records.

2. Security Awareness Statements

It is required that agency policy and procedures relating to personnel security be in written form and made available to all employees. Employees and other individuals allowed to perform duties on behalf of a criminal justice agency in such a manner that may expose them to KCJIS-sensitive information in the course of their duties, to include reserves, interns, volunteers, consultants, vendors and contractors, are required to read the policies and certify in writing that they are aware of and understand them. The policy shall be included in a formal Awareness Statement where employees and other individuals will certify in writing they understand that violations may result in disciplinary action, or, depending on the type of information, may be subjected to civil and criminal penalties including a fine not to exceed $11,000, and may be considered grounds for immediate dismissal.

3. Training regarding the physical security of the KCJIS terminal and the information obtained from it

Your agency training program shall include physical security of the KCJIS system and the information obtained from it. Maintenance of information in an unsecured environment destroys the operator's ability to control the system and permits the entry of erroneous information, the destruction of appropriate information and the unauthorized dissemination of information. Unauthorized access to and use of criminal justice information can cause severe harm to record subjects. Unauthorized access can also jeopardize numerous criminal justice interests including investigative and intelligence gathering activities.

4. Training regarding protection of CHRI from unauthorized use

Every employee who works with criminal history information or works in areas where it is located shall be familiar with applicable security requirements. Employees who are authorized to have access to criminal history information shall assume responsibility for the physical security and protection of the information from unauthorized access, disclosure, modification, dissemination or destruction. An organized training program such as classroom instruction shall be implemented, including initial familiarization and follow-up sessions.

5. Agency specific training in NCIC System Quality Assurance is provided

The agency shall provide training to all terminal operators in regard to the requirements and procedures for entry, maintenance, removal and access of NCIC. Agency specific checklists may be incorporated into the procedures. Compliance with NCIC requirements of complete and accurate entries requires that an agency place specific emphasis on the required documentation, proofing of entries and validation procedures.

6. All full access NCIC operators shall be current in NCIC certification

Full access NCIC operators shall, within six months of employment or assignment, have initial training, be functionally tested and have their certification affirmed in order to

assure compliance with NCIC policy and regulations. Newly hired operators with full access to NCIC are required to receive classroom training followed by certification testing provided by a Kansas Highway Patrol CJIS Trainer/Auditor. Agencies shall notify their respective CJIS Trainer/Auditor to inform them of new operators hired.

Operators shall be functionally retested, via nexTEST, biennially.

7. **All limited access NCIC operators shall be current in NCIC certification**

Limited access operators are persons whose responsibilities include inquiry capability to one or more components of the NCIC system. The operator does not have responsibilities that include making any entries into NCIC. The responsibility for training, functional testing and affirmation of proficiency of these operators according to their level of use, within the first six months of employment, lies with the terminal agency.

Limited access operators shall be functionally retested, via nexTEST, biennially as well.

Part Three - Records Storage Section A: Storage of agency CHRI

1. **CHRI is filed alphanumerically (i.e.; by name, case number, etc.)**

Title 28 does not protect agency records when they are maintained chronologically. Chronological records, those filed by date and/or time, such as police blotters and jail logs are open to the public. Therefore, case files should be filed alphanumerically.

2. **Juvenile justice information is distinguished from adult CHRI by flagging or filing separately**

The regulations regarding dissemination of juvenile records are considerably more restrictive than adult records. Juvenile records shall be "readily distinguishable" to safeguard against improper dissemination.

3. **Record storage and disposal**

All KCJIS-sensitive information shall be securely stored to prevent access by unauthorized personnel. KCJIS-sensitive information shall be disposed of in a manner to prevent access or recovery by unauthorized personnel. Paper copies shall be shredded or incinerated.

Any electronic device shall have a specifically designed computer program to erase the device, or the device shall be degaussed or physically destroyed. Access devices that have KCJIS-sensitive information on them shall have any non-volatile memory components (i.e., hard drives) removed and destroyed.

Part Four – Dissemination

Section A: Protection and Dissemination of KCJIS-sensitive Information

1. Protection of KCJIS-sensitive information

All criminal justice agencies are required to store KCJIS-sensitive information in a manner that prevents unauthorized access. Agencies shall take reasonable precautions to ensure KCJIS-sensitive information will be secure from theft, sabotage, fire, wind, and other natural or manmade disasters.

To protect against unauthorized access, computers must be configured in a way that requires users to log on and authenticate by means of a unique User ID and password.

2. Who can receive KCJIS information

Before KCJIS-sensitive information is disseminated, the person disseminating the information shall ensure the other person is authorized to receive it. A sanction may be imposed on an agency or an agency employee for inappropriate dissemination.

KCJIS-sensitive information shall not be disseminated to non-criminal justice personnel except the following:

a. Any information from the National Weather Service or KHP road reports may be disseminated to anyone by any means.

b. Humanitarian attempts to locate may be disseminated to anyone by any means. **Exception**: Nlets AML (Administrative Message designated to Law Enforcement only) cannot be disseminated.

c. Dissemination of NCIC unrestricted files information is permitted to anyone upon request to confirm the status of a person and/or property, i.e. wanted or stolen, provided that it does not fall under the definition of commercial dissemination. If there are no wants or warrants, Communications Officer may advise as such. If there are wants or warrants, Communications Officer will advise to contact nearest Law Enforcement Agency.

3. How KCJIS information may be transmitted by local criminal justice agencies.

A. Electronic "transmission" of KCJIS-sensitive information

KCJIS-sensitive information shall not be transmitted electronically, in any unencrypted format, except for the following:

a. Information from the National Weather Service or KHP road reports.

b. Kansas humanitarian "attempt to locates", except when indicated it is intended for law enforcement release only.

c. NCIC unrestricted files information solely regarding wanted or stolen status.

d. Driver's license or other photos provided no personal identifying Information (PH) accompanies the photo. Examples of PH include but are not limited to: Driver's License, FBI, KBI or Social Security numbers and/or names.

KCJIS-sensitive information may be transmitted through an approved mobile data computer network that meets minimum encryption requirements, as outlined in the KCJIS Policy and Procedure Manual, to a mobile data access device having a KCJIS assigned mnemonic.

KCJIS-sensitive information may be transmitted by e-mail when both the sending and receiving e-mail boxes belong to one of the approved encrypted domains:

leo.gov
magloclen.riss.net
mocic.riss.net
nespin.riss.net
rocic.riss.net
rmin.riss.net
wsin.riss.net
risstech.riss.net
adg.riss.net
cbi.org
leiu.org
hidta.net
epicmail.riss.net

Agencies are also now allowed to e-mail CJI from one agency to another IF the sending agency can ensure they are utilizing a NIST (National Institute of Standards and Technology) approved encryption program employing a minimum of 128 bit encryption.

Text messaging is prohibited.

B. Transmission of CHRI in audio format

Any electronic device that uses wireless or radio technology to transmit voice data may be used for the transmission of CHRI when an officer determines that there is an immediate need for this information to further an investigation or there is a situation affecting the safety of an officer or the general public.

Codes to disguise the transmission of non-conviction and arrest CHRI shall be used.

C. Fax dissemination of KCJIS-sensitive information

KCJIS-sensitive information may be transmitted by fax if both the sending and receiving agencies have valid criminal justice ORI's.

Internet or wireless fax transmissions are now allowed under the new KCJIS Policy, but only when the encryption standards applied to e-mailing are met.

To prevent non-authorized personnel from viewing the data the sending agency shall call the receiving agency before transmission to ensure the person requesting the KCJIS-sensitive information will be present to receive the data to avoid any inadvertent secondary dissemination.

4. Dissemination of Criminal History Record Information (CHRI)

A. Primary Dissemination

All necessary information, including the requestor and terminal operator's names, is captured from the query and this information is maintained on an automated log at the State level. Therefore, the primary dissemination of criminal history record information, directly to the authorized requestor, does not require the maintenance of a manual log by the local agency.

B. Secondary Dissemination

Secondary dissemination is the sharing of CHRI with authorized individuals outside the requestor's own agency. Any dissemination of this nature must be logged by the original requestor or the party providing the dissemination.

Secondary dissemination logs, whether automated or manual, shall be kept for a minimum of three years any time CHRI is disseminated to another authorized criminal justice agency.

Section B: Interstate Identification Index (III)

1. The agency shall use III for authorized purposes only

A. Purpose Code C

The administration of criminal justice generally means any activity involved in the detection, apprehension, detention and pre-trial release of accused persons. Post trial release, prosecution, adjudication, correctional supervision and rehabilitation of criminals are included.

Other uses for Purpose Code C

Purpose code "C" inquiries shall also be conducted on, but not limited to, vendors, contractors (other than IT contractors), carpet cleaners, janitors,

cooks, interns, persons participating in community ride along programs and volunteers at a confinement facility who are providing social or community services rather than rehabilitative services. Also included are confinement facility visitors, confinement facility inmates and inmates' mailing lists.

Initial domestic violence investigations should be conducted under purpose code "C".

B. Purpose Code J

This purpose code shall be used when the III transaction involves back grounding for employment with a criminal justice agency or the screening of employees of other agencies over which the criminal justice agency is required to have management control.

Other uses for Purpose Code J

Others in this category include, volunteer dispatchers, volunteer data entry clerk, volunteers at a confinement facility who are providing inmate rehabilitation, contract information technology service providers and others deemed to be engaged in the administration of criminal justice.

C. Purpose Code H

Under the Housing Opportunity Extension Act of 1996 local HUD agencies that want to use this service are required to obtain an ORI ending in "Q" from NCIC and enter into an ORI Users Agreement with the serving agency before any transactions may be made. Such transactions are limited to "QH" inquiries only and the housing authority can be advised of nothing more than the possible existence of a criminal history.

D. Purpose Code F

When returning a firearm to its rightful owner, it is highly recommended to conduct a PUR/F III check on the individual to ensure the firearm is not being returned to a subject with a disqualifying felony conviction.

It is also permissible to run a PUR/F III check on individuals pawning firearms.

Background checks on *armed* private security officers should be conducted using purpose code "F".

2. III used for non-criminal justice employment purposes is prohibited

Due to the variance in state laws and policies, III **cannot** be used for non-criminal justice employment purposes.

3. III used for licensing purposes is prohibited

Due to the variance in state laws and policies, III **cannot** be used for licensing purposes.

4. Mandatory use of the Attention Field

The full first and last names of the requesting party followed by a slash or dash and the last three characters of the terminal operator's UserID shall be shown in the Attention Field of all III inquiries.

5. Mandatory use of the Reason Field

A clear and specific reason for accessing criminal history information must be included in the Reason Field of each and every III inquiry.

For a purpose code "C" inquiry, a *criminal investigation case number* may be entered as the reason. In the absence of an appropriate case number however, the reason must be clearly spelled out. The word(s) "investigation", "criminal history", and "interdiction" are unacceptable. A more specific statement is required, such as, "burglary investigation", "drug investigation", "inmate classifications", "inmate mailing list", "inmate visitors list" or "packing an NCIC record entry".

For purpose code "J" inquiries, the reasons of "criminal justice employment" and "law enforcement maintenance employee" would be examples of accepted reason field entries.

6. A procedure for logging secondary dissemination is established

Personnel shall be trained that anytime III information in their possession is shared with any authorized member of another criminal justice agency, the dissemination shall be recorded on a secondary dissemination log. NCIC policy requires, "*Each criminal justice agency receiving a III response shall record any secondary dissemination of any III response to another criminal justice agency or any individual within another criminal justice agency, or to anyone legally entitled to receive such information who is outside the original receiving agency*". After receipt, the person receiving the III information is accountable for what is done with the information they receive. This creates an audit trail from which the recipient can account for their handling of III information in the event there is a question regarding III information in the possession of an unauthorized person.

Secondary dissemination logs are required to be kept for three years but there are obvious advantages to maintaining the information for a longer period of time.

7. Agency does not allow any subject to review his/her own record in III

III shall not be used for remote access to a record to be reviewed or challenged by the subject of the record. Record requests for this purpose shall be submitted in writing either to the FBI Identification Division or the state of record.

Part Five - SecurID Token Compliance

1. Users are following proper log-on and log-off procedures

Users of KCJIS shall log-on and log-off of the system at the beginning and end of their shift. Users leaving their access device for any period of time should either log-off the system or lock the device to prevent any unauthorized use.

2. Token/PIN usage policy

The agency shall follow the Token/PIN Usage Policy as required by the KCJIS Policy and Procedure Manual.

3. Use of token by any other personnel

Each SecurID token is assigned for use by one person. Use of a token assigned to one person by another person is prohibited and constitutes a security violation.

4. Selection of Personal Identification Numbers (PIN's)

Each employee who is issued a token shall be responsible for selecting a PIN of his or her choice. In no case shall an agency assign PIN's to their employees. This constitutes a security violation.

5.Written record of PIN's prohibited

The recording or logging of all PIN's for employees of the agency is prohibited. This type of practice destroys the security for employees and the KCJIS system.

Part Six - Terminal Agency Coordinator (TAC) Training

1. Terminal Agency Coordinator (TAC)

Each terminal agency shall have a Terminal Agency Coordinator. Newly appointed Terminal Agency Coordinators and alternates shall attend formal TAC training conducted by a KHP CJIS Trainer/Auditor at the next available class. Refresher training shall be attended on a biennial basis. (Excluded are agencies with Web Portal access only).

Part Seven - Kansas CHRI Using "KIQ" and "KFQ"

1. Kansas CHRI used for authorized purposes only

The Privacy Act of 1974 requires the maintenance of an audit trail of the purpose of each disclosure of a criminal history record and the recipient of that record. Therefore, inquiries and record requests transmitted to the Kansas Central Repository shall include the purpose for which the information is to be used. The purposes for which

certain agencies may use Kansas CHRI and the appropriate codes for use are the following:

A. **Criminal Justice (C)**

Used for official duties in connection with the administration of criminal justice.

B. **Criminal Justice Employment (J)**

Used when the Kansas CHRI transaction involves employment with a criminal justice agency or the screening of employees of other agencies over which the criminal justice agency maintains management control.

C. **Pre-sentence Investigation (P)** Used by the judicial system for sentencing determination.

2. Use of Kansas CHRI for non-criminal justice employment is prohibited

Per Kansas statutes the KCJIS terminal *cannot* be used to access Kansas CHRI for noncriminal justice employment purposes.

3. Agency is making proper use of the Attention Field

The full first and last names of the requesting party followed by a slash or dash and the last three characters of the terminal operator's UserID shall be shown in the Attention Field on all Kansas CHRI inquiries. Terminal operators shall append the last three characters of their UserID after the requestor's name in the Attention Field on all Kansas CHRI inquiries, even if the requesting party and the operator making the inquiry are one and the same.

Your agency may require further information (i.e., radio or identification numbers) in the Attention Field in addition to the requirements listed.

4. Agency is making proper use of the Reason Field

A clear and specific reason for accessing criminal history information must be included in the Reason Field of each and every Kansas Criminal History Record inquiry.

For a purpose code "C" inquiry, a *criminal investigation case number* may be entered as the reason. In the absence of an appropriate case number however, the reason must be clearly spelled out. The word(s) "investigation", "criminal history", and "interdiction" are unacceptable. A more specific statement is required, such as, "burglary investigation", "drug investigation", "inmate classifications", "inmate mailing list", "inmate visitors list" or "packing an NCIC record entry".

For purpose code "J" inquiries, the reasons of "criminal justice employment" and "law enforcement maintenance employee" would be examples of accepted reason field entries.

5. **A procedure for logging secondary dissemination is established**

Personnel shall be trained anytime Kansas CHRI in their possession is shared with any authorized member of another criminal justice agency; the dissemination shall be recorded on a secondary dissemination log. After receipt, the person receiving the Kansas CHRI is accountable for what is done with the information they receive. This creates an audit trail from which the recipient can account for their handling of Kansas CHRI in the event there is a question regarding the information in the possession of an unauthorized person. Secondary dissemination logs are required to be kept for three years but there are obvious advantages to maintaining the information for a longer period of time.

6. **Agency does not allow any subject to review his/her own record in Kansas CHRI.**

Kansas CHRI shall not be used for remote access to a record to be reviewed or challenged by the subject of the record. Record requests for this purpose shall be submitted in writing to the Kansas Bureau of Investigation.

Part Eight - Kansas Warrant

File Section A: Record Entry

1. **Entry Criteria**

A Kansas warrant record may be entered immediately after; (1) the decision to arrest or authorize arrest has been made; and (2) the entering agency has made the determination to the maximum extent possible if transportation will be authorized.

2. **Transportation limitations shall be entered**

If there is a limitation concerning transportation of the subject, the limitations shall be placed in the transportation text field of the record.

3. **Record may be entered for officer safety purposes**

If the entering agency is absolutely certain the wanted person will not be transported, the record may still be entered for officer safety purposes. The letter "N" is placed in the transportation field and "NOEX" placed as the first four characters in the transportation text field.

4. **Agency makes every effort to enter a complete record**

All available resources shall be checked to obtain personal descriptors and identifiers, which could assist in the positive identification and apprehension of a subject. These resources include but are not limited to agency case files, III, KS CHRI, other states' CHRI, DMV and RJIS.

5. Hyphenated last names shall be separated by a hyphen when entered

The system automatically indexes the last name as entered and indexes the second name so that an inquiry on either the last name or a combination of the last names will result in a hit.

6. Supporting Documentation

Documentation supporting data entered in each field of a Kansas Warrant entry shall be maintained in the case file. This would include the warrant and Kansas Warrant entry worksheet. When supplemental data is received it shall be documented and placed in the case file.

Copies of III, or other forms of CHRI, may be retained in the case file at the agency's discretion.

The supporting documentation for active Kansas Warrant entries shall be easily accessible and not stored in remote areas of the department or buildings outside the agency. This will allow for easier validation of records and confirmation of hits. Agencies that have converted to a paperless records system will not be required to create a paper file on any transactions conducted on these entries for audit purposes. The auditor will prearrange with the agency a mutually agreeable method of gaining access to the case files selected for review in the audit process.

7. Entry Worksheet

An entry worksheet shall be completed and retained in the case file for every Kansas Warrant File entry.

8. Second party check to ensure accurate records

The accuracy of Kansas Warrant records shall be double checked by a second party. This verification shall be completed by someone other than the person making the entry. The second party check shall ensure all available cross checks were made and that the data entered is accurate and matches the supporting documentation. The second party check must be documented on the entry worksheet.

9. If making entries for another agency, their ORI is used

Only the agency that holds the warrant may make a Kansas Warrant File entry. When a serving agency completes an entry for a served agency, with a ORI Users Agreement in place, the ORI of the served agency is to be utilized in the entry.

The only exception is that any criminal justice agency or regional dispatch center may act as a holder of the record for another agency which has no telecommunications equipment and/or does not provide 24/7 service.

When such an entry is made, the agency holding the record may place its own Originating Agency Identifier (ORI) in the ORI field, but only when there is a written agreement between the two agencies that delineates the legal responsibility of each for the record.

Section B: Validations

1. Validation of existing records

Once the determination has been made that the record should remain in the Kansas Warrant File:

a. Access the online web interface located at http://ksmart.kcjis.state.ks.us ; select Warrant Views/Validations from the menu on the left hand side of the page to access the search form necessary to retrieve the records due for validation.

b. All record validations result in the KCJIS usercode of the operator and the current date and time being appended to the record.

c. The most current validation worksheet must be maintained in the case file.

2. Contacting the court and/or prosecutor

The court and/or prosecutor shall be contacted to determine if the warrant is valid and outstanding before the validation is completed.

3. Re-checking all resources for validation

All resources shall be re-checked to ascertain if additional descriptors and/or identifiers have become available that could be added to the original record. If any additional, or
different, data is available, the record shall be supplemented and/or modified during the validation process. Documentation supporting any changes shall be retained in the case file.

Section C: Hit Confirmations

1. Kansas KYQ and KYR formatted messages are used to confirm Kansas Warrant File entries

A fixed format hit confirmation was developed for use by Kansas criminal justice agencies. This message is sent through the Kansas system utilizing a message type for inquiry (KYQ) and response (KYR). When requesting confirmation on a hit or responding to a request for confirmation, it is required that agencies use the "KYQ" and "KYR" respectively.

2. Hit confirmations shall be available 24/7

Every agency that enters records into the Kansas Warrant File shall assure that hit confirmation is available 24/7 either at the entering agency or at another agency through a Holder of Record agreement.

3. Identity of record subject shall be determined before confirmation

The entering agency shall determine the person being inquired upon is identical to the person identified in the record, and that transportation is authorized, before confirming the hit.

4. Response to a hit confirmation request

Each agency is required to respond to a hit confirmation request within ten (10) minutes (Urgent) or one (1) hour (Routine) or advise the requesting agency of a specific amount of time necessary to confirm or reject the hit.

There are no locate procedures for the Kansas Warrant File.

Section D: Record Removal

1. Entering agency shall clear the record entry

The entering agency is responsible for clearing the record entry from the Kansas Warrant File when the subject of the record is in the custody of the entering agency, or they are officially advised the wanted person is in the custody of another agency.

2. Entering agency shall cancel the record entry

The entering agency is responsible for canceling the record entry immediately after being advised that the entry is no longer valid (i.e., warrant is dismissed or recalled).

3. Inquiry by KIC following removal

After removing a Kansas Warrant File record (clear or cancel), the agency shall run an inquiry by KIC number to ensure the record has been successfully removed and retain the printout of the "NO MATCH" response in the case file.

4. Retention of the case file

The supporting case file must be retained until all possible levels of appeal are exhausted or the possibility of a civil suit is no longer anticipated.