Kentucky Noncriminal Justice User Manual

Revised February 14, 2019

TABLE OF CONTENTS

Acronyms	Defined
AFIS	Automated Fingerprint Identification System
CHRI	Criminal History Record Information
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
CSA	CJIS System Agency
CSO	CJIS System Officer
CSP	CJIS Security Policy
COT	Commonwealth Office of Technology
FBI	Federal Bureau of Investigation
ISO	Information Security Officer
IT	Information Technology
KRS	Kentucky Revised Statute
KSP	Kentucky State Police
LASO	Local Agency Security Officer
LINK	Law Information Network of Kentucky
NAC	Noncriminal Justice Agency Coordinator
NCJA	Noncriminal Justice Agency
ORI	Originating Agency Identifier
SAT	Security Awareness Training
SIB	State Identification Bureau
SID	State Identification Number
SOR	Sex Offender Registry
UCN	Universal Control Number

Introduction

This guide was created to assist noncriminal justice agencies that submit fingerprints and receive criminal history record information for noncriminal justice purposes pursuant to authorizations allowed by state and federal law.

What is a Noncriminal Justice Agency (NCJA)?

A NCJA is defined (for the purposes of access to CJI) as an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

What is Criminal Justice Information (CJI)?

Criminal Justice Information is the term used to refer to all of the provided biometric, identity history, biographic, property, and case/incident history data necessary for law enforcement and civil agencies to perform their missions.

What is Criminal History Record Information (CHRI)?

"Criminal History Record Information" means a record compiled by the central repository or identification bureau on an individual consisting of name(s) and identification data, notations of arrests, detentions, indictments, information's, or other formal criminal charges. Criminal history information does not include driver history records or fingerprint records on individuals that may have been submitted for civil or employment purposes. The Kentucky State Police is the repository for criminal history in Kentucky via the Law Information of Kentucky (LINK) program.

CHRI is defined by Title 28 Code of Federal Regulations (CFR) §20.3 as information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. 28 CFR §20.21 further states information is considered CHRI if it confirms the existence or nonexistence of CHRI. CHRI is also described by the FBI CJIS Security Policy 4.1.1 as a subset of Criminal Justice Information (CJI) and is sometimes referred to as "restricted data." Information is considered CHRI if it is transferred or reproduced directly from CHRI received as a result of a national FBI check and associated with the subject of the record. This includes information such as conviction/disposition data as well as identifiers used to index records regardless of format.

Criminal history information does not include driver history records or arrests in which the offender was issued a summons. All CHRI must be supported by a fingerprint submission taken at the time of arrest.

Use of Criminal History Record Information (CHRI)

The FBI is authorized to exchange CHRI with, and for the official use of, authorized officials of the Federal Government, States, cities, and other institutions. CHRI may be made available for use in connection with licensing or employment, pursuant to *Public Law 92-544*, or other federal legislation and for other uses for which dissemination is authorized by federal law. CHRI obtained under such authority may be used solely for the purpose for which the record was requested. When CHRI is needed for a subsequent authorized use, a new record request must be conducted to obtain current information. Subject fingerprints or other approved forms of positive identification shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the III using name-based inquiry and record request messages is not permitted for noncriminal justice purposes, unless otherwise approved by the FBI and/or the Compact Council pursuant to applicable authority.

Agencies must have an Originating Agency Identifier (ORI) number assigned to them as a prerequisite to obtaining fingerprint-based criminal history record. An ORI number is assigned by KSP CJIS Compliance Supervisor/ISO only to agencies that are authorized to obtain a criminal history record check by Kentucky Revised Statute (K.R.S.).

Authorization

Federal

Federal Public Law 92-544 provided for funds to be allocated for the exchange of criminal history identification records for noncriminal justice purposes, pursuant to approved statutes. In 1998, the National Crime Prevention and Privacy Compact Act was passed allowing signatory states to exchange criminal history records for noncriminal justice purposes according to a uniform standard. The 1998 act also established the National Crime Prevention and Privacy Compact Council to regulate and assist in maintaining a method of exchange of criminal history record information which protects both public safety and individual privacy rights. The FBI Criminal Justice Information Services (CJIS) Division houses the largest repository of fingerprint-based criminal history records and is charged with the responsibility and authority to oversee the exchange of such records. Federal laws, regulations, and policies have been formed both to govern the release of information exchanges through the FBI and to require states to regulate access, use, quality, and dissemination of state-held records.

The authority for the FBI to conduct a criminal record check for a noncriminal justice licensing or employment purpose is based upon Public Law 92-544. Pursuant to this law, the FBI is empowered to exchange identification records with officials of state and local governments for purposes of licensing and employment if authorized by a state statute which has been approved by the Attorney General of the United States.

Public Law 92-544 Requirements:

The Attorney General's authority to approve the statute is delegated to the FBI by 28 C.F.R. § 0.85(j). The standards employed by the FBI in approving Pub. L. 92-544 authorizations have been established by a series of memoranda issued by the Office of Legal Counsel, Department of Justice. The standards are:

1. The authorization must exist as the result of legislative enactment (or its functional equivalent);

2. The authorization must require fingerprinting of the applicant;

3. The authorization must, expressly or by implication, authorize use of FBI records for screening of the applicant;

4. The authorization must not be against public policy;

5. The authorization must not be overly broad in its scope; it must identify the specific category of applicants/licensees.

CHRI obtained under this authority may be used solely for the purpose for which the record was requested and shall not be shared with any other agency or entity, even if the agency or entity is authorized to receive CHRI pursuant to its own statutes. When CHRI is needed for a subsequent authorized use, a new record request including fingerprints must be submitted to obtain the most possible current and accurate information.

State

Kentucky's authorization for NCJ access comes from Kentucky Revised Statutes (K.R.S.). Each noncriminal justice agency is required to maintain a signed consent form on each subject of a record check. The form must indicate the K.R.S. authority in which the entity is permitted inquiry of CHRI. The applicable K.R.S. allowing noncriminal justice agencies to access CHRI must be noted in the 'Reason for Fingerprinting' section of the fingerprint card.

Each agency authorized to receive criminal history record information (CHRI) must sign a user agreement. A user agreement is a contractual agreement between the authorized receiving agency and the CJIS Systems Agency (CSA), Department of Kentucky State Police (KSP); it must be signed by the CJSI Systems Officer (CSO) and the appropriate authority at the user agency. The user agreement contains Terms and Conditions which include the following:

***Authority and Purpose*:** The user agreement states the purpose for which criminal justice history information is requested, and the specific authorization granting access to the information. Noncriminal justice agencies are prohibited from using criminal history record information for any purpose other than that for which it was requested.

Local Agency Security Officer (LASO): Pursuant to CSP 3.2.9, the User Agreement requires the appointment of a LASO to act as liaison with the CJIS Systems Agency (Kentucky State Police) to ensure the agency is in compliance with security procedures. LASOs are designated as the point of contact on security-related issues for their respective agencies and are responsible for instituting the CSA incident response reporting procedures at their agency as needed.

***Noncriminal Agency Coordinator (NAC)*:** The chief official of each noncriminal justice agency will designate a NAC to act as the primary contact person for that agency. The NAC should complete ACIC training requirements and shall serve as liaison between the agency and KSP. The NAC should assure all employees are current on training and assist the CJIS Compliance Staff personnel in the audit process. The NAC can also be the LASO.

Training: Agencies are responsible for complying with mandatory training requirements. KSP will provide training or instruction on fingerprint handling and submission for all agencies accessing CHRI. All agency personnel who view or handle CHRI must complete the standard online training via CJIS Online and undergo agency internal training on CHRI security and handling based on the required policies/procedures via the agency LASO.

***Policies/Procedures*:** As part of privacy and security, agencies are required to develop and implement policies and procedures which provide for the security and proper handling of the CHRI. Agencies should also have rules for fingerprint submissions which include proper applicant identification and protecting the fingerprint card from tampering.

***Sanctions/Penalties*:** The user agreement is subject to cancellation by either party with 30 days written notice. KSP reserves the right to suspend service for violations or for investigations of apparent/alleged violations of the user agreement or requirements for access. State and federal civil and/or criminal penalties may apply for misuse of CHRI.

Dissemination of Criminal History Record Information: CHRI must be used solely for the purpose requested and cannot be disseminated outside the receiving departments, related agencies, or other authorized entities.

***Secondary Dissemination*:** All CHRI dissemination outside the receiving agency must be logged and the log shall be retained for a minimum of one year. Secondary dissemination can only be shared between authorized persons/agencies. The log should clearly identify the following:

a) Date of dissemination;
b) Agency employee name requesting;
c) Requesting Agency;
d) Purpose for which information is requested;
e) Specific information being released (i.e., criminal history of name of applicant);
f) Name/signature of the person receiving the request; and
g) Disseminating agency name.

There are two types of submission for noncriminal justice agencies in Kentucky.

1. ***CJI Access*** – CSP 5.12.1 requires proper security measures are followed to authorize any persons with access to CJI. Personnel with CJI access must have a fingerprint-based background check. If a felony record of any kind exists, CJI access shall not be granted.
2. ***Employment*** – Fitness Determination – determination, utilizing CHRI, of whether an applicant is eligible for employment or licensing based upon applicable state or federal law.

In the fingerprint criminal history check process, the agency has a legal authorization to submit applicant fingerprints to KSP. The process takes place between the agency and KSP; the agency submits the prints and the available criminal history record is sent to the agency for review. If there is no criminal history, the KSP and/or FBI Results Report will indicate a negative response. The use of the criminal history results is limited to the sole purpose outlined in the agency's statutory authorization to submit fingerprints. The agency must have an active user agreement on file with KSP and is subject to compliance regulations and periodic audit. The fingerprint criminal history check process is a "point in time" check, and an agency would only see changes to a person's criminal history if the fingerprints were submitted again.

Proper Citing of the "Reason Fingerprinted"

Fingerprint cards can only be submitted for specific purposes under approved authorizations. In the "Reason Fingerprinted" box on the card, agencies are required to specify BOTH the particular purpose the submission (employee, volunteer, professional license type) and the authorizing authority (Kentucky Revised Statute/KRS).

Applicant Identification

Agencies must have established processes for verifying the identity of the applicant at the time of fingerprinting.

The National Crime Prevention and Privacy Compact Council published the Identity Verification Program Guide containing suggestions and best practice recommendations for verifying an applicant's identity and safeguarding the integrity of the fingerprints. A copy of the guide can be downloaded from the FBI website in the Compact Council section. Compact Council recommendations regarding proper identification of applicants include:

• Accept only valid, unexpired photo identification documents as primary proof of identity.

• When accepting secondary identification (i.e. birth certificate, Social Security card), ask for supporting documentation such as a utility bill, bank statement, or mortgage documents.

• Use additional identification data support methods such as:

  - Examine the applicant's photograph on the identification provided and visually compare the picture with the applicant.
  - Compare the physical description on the documentation to the applicant's features (e.g. height, weight, hair and eye color, age, etc.)
  - Request the applicant to verbally provide date of birth, address, etc. and verify the answers with the identification provided.
  - Check the applicant's signature provided in person with a signature on the identification provided.
  - Examine the provided identification to ensure that it has not been altered in any manner.

If the agency uses an outside agency for fingerprinting, then the agency should provide instructions to the applicant to be given to the fingerprint technician. This should include information on how to properly identify the applicant. To ensure the instructions are followed, it is recommended that the instruction form require the fingerprint technician to record (at a minimum) the applicant's name, the type of ID presented by the applicant and the name and company of the fingerprint technician. The form should then be returned to the agency.

Protection of the Fingerprint Card Prior to Submission

Agencies must have established processes for protecting the integrity of the fingerprint card and preventing tampering with the card from the time the prints are taken through the submission to KSP. These procedures establish a process which prevents the applicant from possessing a completed fingerprint card or prevents direct access to the card (such as a sealed envelope system). The processes should also include instructions to fingerprinting personnel as necessary.

Review and Challenge Notification

It is the agency's responsibility to notify applicants of the opportunity and ability to review and challenge a criminal history record.

Per Title 28 Code of Federal Regulations 50.12 (b), whenever an agency submits fingerprints for FBI criminal history record checks, the following actions/disclosures are required:

- The person being fingerprinted must be notified in writing that the fingerprints will be used to check the criminal history records of the FBI.
  - The written notification to the applicant must be provided in a format where the person can read and take a copy with him/her if desired. It is recommended, but not required, that the written notification be presented to the applicant on a document that the applicant is required to sign.
  - Simply stating that the applicant is subject to a "national background check" is NOT sufficient.
- The person being fingerprinted must be informed that they are allowed a reasonable time to complete and challenge the accuracy of the criminal history record. ALL applicants must be advised of this, not just those who dispute an employment/license denial.

    - If the applicant elects to review/challenge the criminal history record, the agency must provide the applicant a reasonable period of time to do so before final denial.
    - The agency should also establish and document what constitutes a reasonable period of time for the review and challenge and any appeals process that is available to the applicant.
- Agencies must notify applicants how to obtain a copy of the FBI record and that the guidelines for these procedures are contained in Title 28 Code of Federal Regulations 16.34.
    - To obtain your FBI criminal history report: https://www.fbi.gov/services/cjis/identity-history-summary-checks
    - To obtain your State criminal history report: http://kentuckystatepolice.org/forms/background-check-forms/

Fees

For General Public, State, and Federal background checks: Kentucky Revised Statute (K.R.S.) 17.185 enables the Kentucky State Police to charge a processing fee for access to criminal history record information for noncriminal justice purposes. For current fee information, see the KSP website; Records (Backgrounds Checks).

For FBI Only background checks: 28 C.F.R. § 20.31 allows the FBI to collect fees for noncriminal justice purposes.

K.R.S. 16.068, 65.068, and 70.095 also enables state, local, and county agencies that take fingerprints and/or photographs needed to perform background checks to also charge a fee for this action.

Guidelines for Preparation of Fingerprint Cards

https://www.fbi.gov/file-repository/guidelines-for-preparation-of-fingerprint-cards-and-association-criminal-history-information.pdf/view

Security of Criminal History Record Information

Noncriminal justice agencies must have written policies and procedures regarding access, use, dissemination, and disposal of CHRI. These policies and procedures must be submitted to the CJIS Compliance Staff or the CJIS Information Security Officer (ISO) upon request.

Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration, or misuse. Using the requirements in the CJIS Security Policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange. The agency must have a policy which ensures that CHRI is only used for the purpose for which it is requested.

The agency policy should include:

- Defining who is authorized to access CHRI
- Restricting access to only Authorized Personnel
- Proper security of CHRI from receipt through destruction
- Communication of rules to appropriate personnel
- Communication among Authorized Personnel
- Communication with the applicant concerning CHRI
- Retention procedures
- Destruction procedures

The agency must also have policies in place to prevent the unauthorized disclosure of CHRI. The agency policy to prevent unauthorized disclosure should include:

- Access-limited storage
- Physical security of CHRI
- Revocation of access privileges for terminated employees or those removed from Authorized Personnel List

The agency must have a formal disciplinary process in place for misuse of CHRI. If the agency has a general misconduct or disciplinary policy, the agency would need to demonstrate how this policy would be applied in the event of a misuse situation.

If applicable, the agency must have policy in place governing the electronic storage of CHRI. This includes:

- Monitoring and restricting access to databases containing CHRI
- Physical/technical safeguards to protect the access and integrity of the CHRI
- Reporting, response, and handling capability for information security incidents

Physical media shall be securely disposed of when no longer required, using formal procedures shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall only be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

If the agency utilizes electronic storage, the agency shall sanitize, by overwriting at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. The agency must have these procedures written in the agency's policy.

The exchange of the CHRI is subject to immediate cancellation if dissemination is made outside the receiving departments or related agencies and if CHRI is used for any other reason that is not stated in Kentucky law. Furthermore, depending upon the nature of the offense and the identity of the offender, federal or state crimes may be charged for the willful, unauthorized disclosure of CHRI. Misuse of the CHRI can be a misdemeanor or felony depending on the circumstances.

Penalties for Misuse of CHRI:

- 28 U.S.C. § 534 (b)
- Public Law 92-544
- 28 C.F.R. § 20.33(b) and (d)
- KRS 15.520

Agencies are required to establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity. The agencies must have these procedures written in the agency's security policy. This includes maintaining the criminal history record information in a secure location that is not readily accessible to individuals not authorized to see it.

Physical Security includes:

- Protection of information subject to confidentiality
- Limitation of visitor access to controlled areas
- Prevention of social engineering
- Positioning of computer and system devices (lap tops, cellular phones, I-pads, or any kind of hand held devices used to access, process or store CHRI media) in such a way that prevents unauthorized personal gaining physical or visual access.
- Locking of rooms, areas, or storage containers where CHRI media is accessed, processed and/or stored

Electronic Security includes:

- Protection of information subject to confidentiality
- Password use and management Protection from viruses, worms, Trojan horses and other malicious code
- Appropriate use and management of e-mail, spam and attachments
- Appropriate web use
- Use of encryption; for transmission of sensitive/confidential information through electronic means.
- Backing up electronic media on a regular basis.

The IT personnel's responsibility to install:

- Protection from viruses, worms, Trojan horses, and other malicious code through electronic scanning and updating definitions.
- Provide data backup and storage through centralized and decentralized approaches, when applicable.
- Provide timely application of system patches as part of configuration management.
- Provide access control measures.
- Provide protection measures for agency Network infrastructure.

In addition to the required fingerprint-based background check, all persons directly associated with the accessing, maintaining, processing, dissemination or destruction of CHRI shall be trained. The training shall provide employees with a working knowledge of federal and state regulations and laws governing the security and processing of criminal history information. Employers are responsible for ensuring that their personnel receive such training within six (6) months of employment or job assignment. The CSP requires recertification every two (2) year for noncriminal justice agencies personnel. Users should contact the agency's NAC to be setup for training. The CJIS Security Training can be located at https://www.cjisonline.com

User Forms

See **Forms** under NJCA icon

Levels of Training

There are 4 Levels of CJIS Security Training:

Level 1 Security Awareness Training Personnel with Un-escorted Access to Physically Secure Location (This level is designed for people who have access to a secure area but are not authorized to use FBI Criminal History Result. Example: Custodian Staff; Maintenance Staff).

Level 2 Security Awareness Training All Personnel with Access to CJI; *including Criminal History* (Example: Personnel that views, handles, knowledge or access to storage locations of where the FBI Criminal History Result).

Level 3 Security Awareness Training Personnel with Physical and Logical Access *to CJI.* (Example: This level is designed for personnel who typically have access to query, enter, or modify Criminal History Information data in an electronic format.)

Level 4 Security Awareness Training Personnel with Information Technology *Roles* (This level is designed for all information technology personnel including system administrators, security administrators, network administrator, etc. Example: Computer Maintenance Personnel).

Security Training Minimums

At a minimum, the following topics shall be addressed as baseline security awareness training for all authorized personnel with access to CHRI:

a) Rules that describe responsibilities and expected behavior with regard to CHRI usage.
b) Implications of noncompliance. Incident response (Points of contact; Individual actions).
c) Media protection.
d) Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity.
e) Protect information subject to confidentiality concerns — hardcopy through destruction.
f) Proper handling and marking of CHRI.
g) Threats, vulnerabilities, and risks associated with handling of CHRI.
h) Social engineering.
i) Dissemination and destruction.

There has been an increase in the number of accidental or malicious computer attacks against both government and private agencies, regardless of whether the systems are high or low profile.

Noncriminal Justice Agencies shall establish an operational incident handling policy and procedure for instances of an information security incident of physical and/or digital CHRI media. Agencies policies must include plans for adequate preparation, detection, analysis, containment, recovery, and user activities.

Preparation – firewalls, virus detection, malware/spyware detection, security personnel, and locked doors to prevent unauthorized access.

Detection – monitoring preparation mechanisms for intrusions such as: spyware, worms, and unusual or unauthorized activities, etc. can include building alarms and video surveillance.

Analysis – identify how an incident occurred and what systems or CHRI media were compromised.

Containment – security tools utilized or an agency plan to stop the spread of the intrusion.

Eradication – removal plan of the intrusion before the system is restored and steps taken to prevent reoccurrence.

Recovery – the ability to restore missing files or documents.

The agency must track, document, and report incidents to appropriate agency officials and/or authorities.

LASO's are designated as the point of contact on security-related issues for their respective agencies and LASOs are responsible institute the CJIS System Agency (CSA) incident response reporting procedures at their agency as needed.

Agency policy must be submitted to the Information Security Officer (ISO). Any incidents must be documented using the Incident Response form and must be submitted to the ISO.

Forms

See **Forms** under NJCA icon

For agencies that store CHRI results electronically, the agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. A copy of this must be submitted to the Information Security Officer (ISO) for approval.

The network topological drawing shall include the following:

1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
3. "For Official Use Only" (FOUO) markings.
4. The agency name and date (day, month, and year) drawing was created or updated.

Forms

See **Forms** under NJCA icon

For agencies that store CHRI electronically, proper encoding of information is required. Encryption does not itself prevent interference, but denies content to a would-be interceptor.

1. Encryption shall be a minimum of 128 bit.
2. When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via cryptographic mechanisms (encryption).
3. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected via cryptographic mechanisms (encryption).
    a) When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:
        i. Be at least 10 characters
        ii. Not be a dictionary word.
        iii. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.
        iv. Be changed when previously authorized personnel no longer require access.
    b) Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases. A single passphrase may be used to encrypt an entire folder or disk containing multiple files. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied.
4. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

    Note 1: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete.

    Note 2: While FIPS 197 (Advanced Encryption Standard) certification is desirable, a FIPS 197 certification alone is insufficient as the certification is for the algorithm only vs. the FIPS 140-2 standard which certifies the packaging of an implementation.

    EXCEPTION: When encryption is used for CJI at rest, agencies may use encryption methods that are FIPS 197 certified, 256 bit as described on the National Security Agency (NSA) Suite B Cryptography list of approved algorithms.
5. For agencies using public key infrastructure technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall:

    a) Include authorization by a supervisor or a responsible official.
    b) Be accomplished by a secure process that verifies the identity of the certificate holder.
    c) Ensure the certificate is issued to the intended party.

CJIS Security Policy 5.11 Formal Audits authorize the FBI CJIS Division to conduct security audits of Kentucky State Police, the state's CJIS System Agency (CSA), and the KSP's LINK networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. To assess noncriminal justice agencies compliance with the CJIS Security Policy, the KSP CJIS Compliance Staff hall:

- At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.
- In coordination with the CSA, establish a process to periodically audit all NCJAs, with access to CJI, in order to ensure compliance with applicable statutes, regulations and policies.
- Have the authority to conduct unannounced security inspections.

In other words, Noncriminal Justice Agencies (NCJA) that are authorized to receive CHRI for noncriminal justice purposes are subject to audit to ensure compliance with state and federal rules regarding fingerprint submissions and CHRI use. The NCJA may be audited every three years in order to assess compliance with state and federal policies and regulations. The NCJA may also be audited as part of triennial FBI audits of the Kentucky State Police.

For additional assistance pertaining to the Audit process please email cjistraining@ky.gov