Arkansas Crime Information

Noncriminal Justice Agency Guide

rev. 4/01/2019

Contents

Acronym Glossary

Acronym	Term
ACIC	Arkansas Crime Information Center
ASP	Arkansas State Police
CEO	Chief Executive Officer
CHRI	Criminal History Record Information
CJI	Criminal Justice Information
CJIS	Criminal Justice information Services
CSP	CJIS Security Policy
CSA	CJIOS System Agency
FBI	Federal Bureau of Investigation
INA	Information Network of Arkansas
LASO	Local Agency Security Officer
NAC	Noncriminal Agency Coordinator
NCJA	Noncriminal Justice Agency
ORI	Originating Agency Identifier
SIB	State Identifications Bureau
SID	State Identification

Introduction

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

Overview & History

Federal Public Law 92-544, passed by Congress in October 1972, 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 exchanged through the FBI and to require states to regulate access, use, quality, and dissemination of state-held records.

Arkansas

Arkansas Code Annotated 12-12-1001, 12-12-1501 through 1513, and 12-12-1601 through 1610 allows the release of Arkansas noncriminal justice criminal history background information to entities that have the signed consent of the subject of the record. The release form on file with the employer, service provider or third party must indicate that the employer or Service Provider/Third Party Agent on behalf of the employer or subject shall have the authority to request the criminal background check. Arkansas Crime Information Center (**ACIC**) and the Arkansas State Police will hold the third party responsible for any inquiries. Arkansas Crime Information Center (**ACIC**) will conducts the audits.

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 **ACIC** to agencies that are only authorized to obtain a criminal history record check by Arkansas Code Annotated.

Policy references:

- Title 28, U.S.C., Section 534 (a) (4)
- Title 42, U.S.C., Section 14616, Article IV (c) and Article V (a) and (c)
- Title 42, U.S.C., Section 14616, Article IV (c) and Article V (a) and (c) Title 28, C.F.R., Section 50.12 (b)

 Title 28, C.F.R., Part 901
 CJIS APB “Concept for the Exchange of Criminal History Records for Noncriminal Justice Uses by Means of the III”, Section B.

What is Criminal History Record Information?

“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. This record also includes any dispositions of these charges, as well as notations on correctional supervision and release. 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 Arkansas Crime Information Center (**ACIC**) is the repository for criminal history in Arkansas.

Based on Arkansas law the only information released based on a noncriminal justice criminal records inquiry is:

Any Arkansas felony arrest within the last three years that has not gone to court.
Any Arkansas felony conviction.
Any Arkansas misdemeanor conviction.
Whether the person is a registered sex offender (level 1 through 4).
In certain cases sealed offenses are also released for licensing or employment purposes.

The FBI criminal history record information response could contain more or less information than is on the Arkansas response.

Reason Fingerprinted Field and Purpose Code Usage

The Privacy Act of 1974 requires that the FBI's CJIS Division keep an accurate accounting of the purpose of each disclosure of a criminal history record and the recipient of that record. All name-based III inquiry and record request messages must include the correct purpose code for which the CHRI is to be used. All fingerprint-based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used. In addition, all users are required to provide the reason for all name-based and fingerprint-based III transactions upon request by CJIS Systems managers, administrators, and representatives.

Policy references:
 Title 5, U.S.C., Section 552a, (c) (1) (A)
 III/NFF Operational and Technical Manual, Chapter 2, Section 2.1

User Fees

To access noncriminal justice criminal history record information through the Arkansas State Police for noncriminal justice purposes, an entity must have an account with the Information Network of Arkansas (**INA**) to submit their request and receive an electronic response. See cost on https://www.ark.org/criminal/index.php.

If an entity does not have an on-line account with **INA**, you can still mail-in a request. The cost is $25.00 each.

User fees are generally set by law and are subject to change.

Agency User Agreement

Each agency authorized to receive criminal history record information (**CHRI**) must sign a user agreement. A user agreement (See Appendix A) is a contractual agreement between the authorized receiving agency, Arkansas State Police, and Arkansas Crime Information Center; it must be signed by the **ASP**, **ACIC** 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 nature of the requesting organization, the purpose for which criminal justice history information is requested, and the specific authorization granting access to the information. **It is prohibited for noncriminal justice agencies to use criminal history record information for any purpose other than that for which it was requested.**

Local Agency Security Officer (**LASO**): The user agreement requires the appointment of a **LASO** to act as liaison with **ACIC** to ensure the agency is in compliance with security procedures. (See Appendix B)

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 **ACIC**. The **NAC** should assure all employees are current on training and assist **ACIC** personnel in the audit process.

Training: Agencies are responsible for complying with mandatory training requirements. ASP 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 (CJIS Online) and undergo agency internal training on CHRI security and handling based on the required policies/procedures.

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. **ACIC and ASP** 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. If passing CHRI to a third party contractor, for the administration of noncriminal justice, the Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the III System and CHRI are not compromised.

All dissemination outside the receiving agency must be logged (See Appendix D and E), and the log shall be retained for a minimum of one year. 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 of the person receiving the request; and
g) Disseminating agency name.

Policy references:

- Title 28 CFR Part 906
- Title 28 CFR 50.12
- Title 28 USC 534

Security of Criminal History Record Information

Noncriminal justice agencies must have written policies and procedures regarding access, use, dissemination, and disposal of CHRI. The auditor will review the agency's required privacy and security policies and procedures and any documents/processes related to security of CHRI.

Disposal of CHRI

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

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 agencies must have these procedures written in the agencies policy. .

Physical Security

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 agencies 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

Personnel Security

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 and every two (2) years thereafter.

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.

Misuse of CHRI

The exchange of the CHRI is subject to CANCELLATION if dissemination is made outside the receiving departments or related agencies and if CHRI is used for any other reason that not stated in the Arkansas state 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 is a misdemeanor or felony depending on the circumstances.

Penalties for Misuse of CHRI

Arkansas Code Annotated 12-12-212 and12-12-1002(b).
- Title 28, U.S.C., § 534,
- Pub. L. 92-544
- Title 28, CFR, 20.33(d)

Applicant Notification, Privacy Right Statement, and Record Challenge

Applicants who are the subject of a national fingerprint-based criminal history record check for a noncriminal justice purpose, have certain rights which are discussed below.

Applicants must be provided written notification that the applicant's fingerprints will be used to check the criminal history records of the FBI. The notification must be kept for the lifetime of the criminal history record information.

Applicants must be provided written notification of the Privacy Right Statement. The FBI's acquisition, preservation, and exchange of fingerprints and associated information is generally authorized under 28 U.S.C. 534. Depending on the nature of your application, supplemental authorities include Federal statutes, State statutes pursuant to Pub. L. 92-544, Presidential Executive Orders, and federal regulations. Providing your fingerprints and associated information is voluntary; however, failure to do so may affect completion or approval of your application.

Principal Purpose: Certain determinations, such as employment, licensing, and security clearances, may be predicated on fingerprint-based background checks. Your fingerprints and associated information/biometrics may be provided to the employing, investigating, or otherwise responsible agency, and/or the FBI for the purpose of comparing your fingerprints to other fingerprints in the FBI's Next Generation Identification (NGI) system or its successor systems (including civil, criminal, and latent fingerprint repositories) or other available records of the employing, investigating, or otherwise responsible agency. The FBI may retain your fingerprints and associated information/biometrics in NGI after the completion of this application and, while retained, your fingerprints may continue to be compared against other fingerprints submitted to or retained by NGI.

Routine Uses: During the processing of this application and for as long thereafter as your fingerprints and associated information/biometrics are retained in NGI, your information may be disclosed pursuant to your consent, and may be disclosed without your consent as permitted by the Privacy Act of 1974 and all applicable Routine Uses as may be published at any time in the Federal Register, including the Routine Uses for the NGI system and the FBI's Blanket Routine Uses. Routine uses include, but are not limited to, disclosures to: employing, governmental or authorized non-governmental agencies responsible for employment, contracting, licensing, security clearances, and other suitability determinations; local, state, tribal, or federal law enforcement agencies; criminal justice agencies; and agencies responsible for national security or public safety.

They are allowed a reasonable opportunity to challenge the accuracy of the criminal history record information. (ALL applicants must be advised of this, not just those who dispute an employment/license denial or who feel their CHRI is incorrect). If the applicant elects to challenge the criminal history record information, 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.

For a copy of an Arkansas criminal history record:

The individual can contact Arkansas Crime Information Center (**ACIC**) at (501) 682-7444 or Arkansas State Police at (501) 618-8000.

For a copy of an FBI criminal history record:

U.S. Department of Justice Order rules allow the subject of an FBI record to request a copy of his/her own record. The individual may submit fingerprints, an Applicant Information Form, and payment directly to the FBI according to the procedures in Title 28 Code of Federal Regulations §16.34.

FBI website for information about record review and challenge: https://www.fbi.gov/services/cjis/identity-history-summary-checks

More information on how to review and challenge an FBI criminal history record can be found at https://www.fbi.gov/services/cjis/identity-history-summary-checks

Chain of Custody

The National Crime Prevention and Privacy Compact Council (Compact Council) is a 15-member body of local, state, and federal governmental officials, which prescribes system rules and procedures for the effective and proper operation of the Interstate Identification Index (III) for noncriminal justice purposes. (See Appendix F)

In recent years, the demand for fingerprint-based background checks for noncriminal justice purposes has increased. Fingerprinting agencies and contractors alike have expressed concern that applicants with a criminal history record may have someone pose as the applicant for fingerprinting purposes. Based on the Compact Council's Best Business Practice, it is recommended to request and obtain photographic identification when capturing an individual's fingerprints. Do not provide a completed fingerprint card to the applicant to submit directly, as the applicant could alter the card.

If agencies allow its applicants to be fingerprinted at a law enforcement agency or a nearby fingerprint service company, the agency must supply the applicant with a 9x12 brown mailing envelope containing a fingerprint card and a "Fingerprint Verification Form" (See Appendix G and H) which contain instructions and a section which must be filled out by the fingerprint technician. The instructions tell the fingerprint technician to request a valid, unexpired government-issued photo ID and to compare the physical descriptors on the photo ID to the applicant. Once the applicant has been fingerprinted, the instructions tell the fingerprint technician to put the fingerprint card and the completed Fingerprint Verification Form into the

envelope and seal it. The technician must write his or her name or identification across the edge of the seal before returning the envelope to the applicant. The applicant then must deliver the envelope with the seal intact to the agency.

Outsourcing

Outsourcing incorporates the process of a third party to perform noncriminal justice administrative functions relating to the processing of criminal history record information (**CHRI**) obtained from the Interstate Identification Index (III), subject to appropriate controls, when acting as a Noncriminal Justice Agency for a governmental agency or other authorized recipient of CHRI. The Noncriminal Justice Agency should provide ACIC written permission to outsource and ACIC will approve or disapprove with a letter and returned approval to the agency.

The Compact Council published a Final Rule in the Federal Register regarding a Security and Management Control Outsourcing Standard, (See Appendix I) which became effective December 15, 2005. The goal of the Outsourcing Standard is to permit the outsourcing (delegation of non-core operations from internal production to an external entity specializing in the management of that operation) of noncriminal justice functions related to processing criminal history record information obtained from III. The Outsourcing Standard permits a governmental agency or other authorized recipient of criminal history record information to select a private or governmental agency to perform these noncriminal justice administrative functions on behalf of the governmental or authorized agency, subject to appropriate controls.

The Outsourcing Standard establishes minimum standards to ensure that security and privacy requirements are satisfied while CHRI obtained from the III is under the control or management of a third party. The contracting parties may not reduce these minimum standards; however, they may adopt more strict standards than required. To ensure agencies follow these minimum standards, the Outsourcing Standard provides that contracts and agreements authorized by this rule "shall incorporate by reference a Security and Management Control Outsourcing Standard approved by the Compact Council after consultation with the United States Attorney General".

The Outsourcing Standard identifies duties and responsibilities for adequate security controls between the authorized recipient and the contractor in order to maintain the security, accuracy, and reliability of the III system and criminal history record information. Arkansas governmental agencies that obtain national criminal history record checks for noncriminal justice purposes under an approved Public Law 92-544 statute may utilize the Compact Council's Outsourcing Standard to permit a contractor or contractors to perform the administration of noncriminal justice functions associated with national criminal history records on behalf of the authorized government recipient. The Outsourcing Standard may require additional stricter requirements on the contractors performing noncriminal justice functions. This includes forwarding the FBI record to a third party subcontractor to determine employment or licensing eligibility at the lowest agency level. (See Appendix J)

Training

Agencies are responsible for complying with the mandatory training requirements. All agency personnel who view, handle or access to storage locations of CHRI must complete basic security awareness training. This training must be completed within thirty (30) days of initial assignment. The CSP requires recertification every two (2) year for noncriminal justice agencies personnel and the Out Sourcing Standard requires recertification training annually (yearly) for noncriminal justice agency vendors.

The CJIS Security Training can be located at www.cjisonline.com. Users should contact the agencies NAC to be setup for 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 FBI Criminal History Result (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 Criminal History Information.
(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:

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

For more information on the ACIC Training Policy, please visit
http://www.acic.org/Websites/acic/images/pdfs/Training_Policy2015.pdf

Incident Response

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.

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. (See Appendix K)

Agencies shall:

Establish an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities;
Track, document, and report incidents to appropriate agency officials and/or authorities.

Configuration Management

Access Restrictions for Changes

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified

and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

Network Diagram

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.

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.

Encryption

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).
EXCEPTIONS: See Sections 5.5.7.3.2 and 5.10.2.

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. 8/4/2014 CJISD-ITS-DOC-08140-5.3 55
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.

Audit

Agencies which submit fingerprints for criminal history checks are subject to audit to ensure that they are in compliance with state and federal rules regarding fingerprint submissions and CHRI use.

The noncriminal justice agency will be audited every 3 years in order to assess compliance with state and federal policies and regulations. **ACIC** personnel conduct the audits. The FBI conducts triennial audits of the state of Arkansas as a part of the audit will visit a selection of noncriminal justice agencies

A routine audit is a scheduled review of the agency's compliance with the Noncriminal Justice Compliance requirements. **ACIC** will send out a written notification approximately 30 days in advance of the planned audit date. The letter will describe the audit process and provide the contact information of the assigned auditor. The notification letter will state whether the agency is scheduled for an in-person audit also included will be a pre-audit Questionnaire.

The auditor will conduct a complete file review of the agency prior to the audit interview. All documentation relating to general administration, fingerprint submissions, privacy and security, and training will be reviewed at the audit interview. The Noncriminal Justice Agency will be asked to complete a questionnaire as part of the pre-interview process.

After an audit has been completed, the auditor will provide the agency with a written report which will either denote complete compliance or will contain recommendations for corrective actions to bring the agency into compliance. Auditors are available to discuss specific concerns and to offer training to assist the agency in this process.

A directed audit is an administrative review triggered as a result of an incident or allegation of possible misuse of CHRI. Most issues of misuse stem from instances of improper and/or unauthorized dissemination of criminal history record information to unauthorized individuals or agencies.

ACIC may conduct a directed audit of an agency if it:
Receives a complaint from an agency or individual alleging misuse of CHRI.
Becomes aware of agency actions which may constitute a misuse of CHRI.
Becomes aware of agency actions which may be a violation of the user agreement terms.

ACIC Field Agent will contact the agency's **NAC** and arrange to conduct a review of the agency's process and actions which may have resulted in a misuse. If **ACIC** cannot reach the **NAC** within a reasonable period of time, the Noncriminal Justice supervisor, agency CEO, or other administrator will be contacted.

The review by **ACIC** Field Agent is designed to detect process issues which may result in noncompliant actions by an agency. Areas which will be audited are the same ones that are checked during a routine audit; in addition, auditors may focus on the policies, procedures, process, and actions most closely related to the allegation. **ACIC** Field Agent will ask questions regarding the circumstances surrounding the allegation to determine if/how the incident occurred and what actions might be required to prevent a repeat of any misuse. The **NAC** should be present for the audit as well as any other personnel the agency deems necessary. Following the directed audit, **ACIC** Field Agent will prepare a written report of his/her findings. If compliance issues are detected, the report will contain recommendations and/or specific requests in order to bring the agency into compliance so that it can continue to utilize the fingerprint-based background check

process through Arkansas State Police. The agency will be required to respond in writing regarding its corrective actions in the areas of concern.

A directed audit does not replace a routine audit. If a directed audit finds issues which require correction, an agency may be scheduled for a routine audit after a specified period of time in order to reassess agency compliance.

Compliance Review

This subsection discusses the general compliance requirements for each of the areas reviewed by auditors: general administration, fingerprint submissions, privacy and security, and training. Each part contains a short explanation of the requirements and may reference different resources or areas of the guide which an agency may refer to for more information.

General Administration

The general administration section of an audit reviews the basic information on file for the agency for completeness, accuracy, and compliance with current regulations.

1.) User agreement:

The user agreement is the contractual agreement between the user agency and Arkansas State Police and Arkansas Crime Information Center that allows Arkansas State Police to provide CHRI upon submission of fingerprints. Changes to the authorization, purpose, or signatory to the agreement all may be reasons that the agreement needs to be updated.

2.) Authorized Personnel List

The **NAC** is responsible for maintaining an updated Authorized Personnel List on file with **ACIC**. The Authorized Personnel List contains those individuals whom the agency has identified as authorized to access, handle, and/or destroy CHRI. The authorizations are based solely on the agency's determination, but should be limited to the minimum number of personnel necessary. **ALL** personnel who view, handle, use, disseminate, or dispose of CHRI **MUST** appear on the list; the list will be checked at every audit.

3.) Agency File Information

The **NAC** should inform **ACIC** of changes in the CEO, the ASC, or any relevant business information (agency name changes, mailing/physical address changes, etc.). The auditor will check that all the information on file at **ACIC** is current. Make changes as they occur – don't wait for an audit!

4.) Authorization and Purpose

Each fingerprint submission access is for a specific purpose and is pursuant to a specific authorization. Fingerprints cannot be submitted for any other purpose than that which is obtained in the agency's authorization. Agencies may have more than one authorization, allowing them to submit fingerprints for multiple purposes. The auditor will check all the agency's authorizations and verify each purpose. A change to an agency's authorization may invalidate the entire user agreement; if the NAC becomes aware of a change in the authorization for access (e.g., change in the authorizing city ordinance, new state statute, etc.), he/she needs to contact the **ACIC** immediately to update the user agreement and, if necessary, submit the new authorization to **ACIC**.

Fingerprint Submissions

The auditor will review the agency's entire fingerprint submission process covering properly filling out the cards, applicant identification, processes to protect the fingerprint card from tampering, and notifications and disclosures to the applicant.

FBI Applicant Privacy Rights Notifications

Any agency which submits fingerprints for FBI criminal history (federal check) is required to advise applicants of the following PRIOR to submitting the fingerprint card to the FBI (via Arkansas State Police):

Applicants must be notified in writing that their 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 applicant can read and take a copy with them if they desire.
Informing all applicants that they are allowed a reasonable opportunity to complete and challenge the accuracy of the criminal history record before final denial.
Agencies must notify applicants how to obtain a copy of the FBI and Arkansas record and that the guidelines for these procedures are contained in 28 CFR 16.34

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, license type) and the authorizing authority (statute number, city ordinance number, executive order number).

Applicant Identification

Agencies must have established processes for verifying the identity of the applicant at the time of fingerprinting. The auditor will check for procedures which include:

- Informing fingerprinting personnel of the identification requirement.
- Requiring photo identification at the time of fingerprinting.

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 **ASP**. The auditor will look for procedures which establish either 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.

Privacy and Security

Noncriminal justice agencies must have written policies and procedures regarding access, use, handling, dissemination, and destruction of CHRI. The auditor will review the agency's required privacy and security policies and procedures and any documents/processes related to security and dissemination of CHRI.

The agency must have a process which ensures that CHRI is only used for the
Purpose for which it is requested.

The agency must have processes in place for the proper access and handling of CHRI.
Access includes:

- Defining who is authorized to access CHRI

- Restricting access to only Authorized Personnel
- Handling rules
- Proper security of CHRI from receipt through destruction
- Communication rules
- Communication among Authorized Personnel
- Communication with the applicant concerning CHRI
- Secondary dissemination procedures
- Retention procedures
- Destruction procedures

The agency must have processes in place to prevent the unauthorized disclosure of CHRI. Prevention of unauthorized disclosure includes:

- Access-limited storage.
- Not leaving CHRI unattended when it is not physically secured.
- Revocation of access privileges for terminated employees or those removed from the 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/activated in the event of a misuse situation.

If applicable, the agency must have processes in place governing 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.

Training

The auditor will review the agency's training documentation to check if Authorized Personnel have received both the mandatory CJIS Online training and the agency's internal process training. All personnel with access are required to be trained in the agency's internal privacy and security processes.

1) All Authorized Personnel must be trained in the online security and awareness (CJIS Online) training within six months of hire (or of being placed on the Authorized Personnel List) and then every two years thereafter.

2) All Authorized Personnel must receive the agency's internal training on the access/use/handling/ dissemination/ destruction procedures every two years. The agency's training should also cover the state, federal, and agency consequences for misuse of criminal history. Auditors will ask to view an outline of the agency's training and any reference policies to assess the training topics.

3) All Authorized Personnel must sign an Acknowledgement Statement acknowledging the notification of the penalties for misuse of CHRI. (See Appendix L)

Authorized Personnel training must be logged on the **NCJA** Training Documentation Form (or equivalent) and the documentation must be available for inspection by auditors. (See Appendix M)

Appendix A – Agency User Agreement

http://www.acic.org/Websites/acic/images/pdfs/Agency-Agreement-between-ACIC-State-Police-and-the-agency.pdf

Appendix B – LASO Form

http://www.acic.org/Websites/acic/images/pdfs/LASO-Form.pdf

Appendix C – NAC Form

http://www.acic.org/Websites/acic/images/pdfs/NAC-Form.pdf

Appendix D – Dissemination Log

http://www.acic.org/Websites/acic/images/pdfs/Dissemination-Log.pdf

Appendix E- Dissemination Form

http://www.acic.org/Websites/acic/images/pdfs/CHRI-Dissemination-Form.pdf

Appendix F – Identity Verification Program Guide

http://www.acic.org/Websites/acic/images/pdfs/Identity-Verification-Guide.pdf

Appendix G – Fingerprint verification Form

http://www.acic.org/Websites/acic/images/pdfs/Fingerprint-Verification-Form.pdf

Appendix H – Live Scan Fingerprint Form

http://www.acic.org/Websites/acic/images/pdfs/Live-scan-Fingerprint-Verification-Form.pdf

Appendix I – Security and Management Control Outsourcing

https://www.fbi.gov/file-repository/federal_outsourcing-guide.pdf/view

Appendix J – Incident Response Form

http://www.acic.org/Websites/acic/images/pdfs/SECURITY_INCIDENT_RESPONSE_FORM-_Appendix_J_Oct_2016.pdf

Appendix K – Acknowledgement Statement Form

ACKNOWLEDGEMENT STATEMENT OF MISUSE

All Authorized Personnel are made aware of the guidelines, consequences and liabilities that could occur from unauthorized use of criminal justice information and criminal history record information. Employees are advised of the following:

- Give a criminal history record information (CHRI) to someone who is not authorized to receive it.
- Allowing unauthorized access to criminal history record information (CHRI).
- Using criminal history record information (CHRI) for any other purpose other than stated in the Arkansas statute.
- Access to criminal justice information (CJI) and criminal history record information (CHRI) via submitted fingerprints could be suspended or cancelled for violation of security and/or violation of the terms and conditions in the User Agreement.
- Misuse of the CHRI is a misdemeanor or felony depending on the circumstances of the release

Penalties for Misuse of CHRI
Arkansas Code Annotated 12-12-212 and12-12-1002(b).
- Title 28, U.S.C., § 534,
- Pub. L. 92-544
- Title 28, CFR, 20.33(b)

I acknowledge that I have been advised of the consequences of misuse of criminal justice and criminal history record information.

_____
Employee Name (Print)

_____ _____
Employee Signatures Date

Appendix L – Training Document Form

http://www.acic.org/Websites/acic/images/pdfs/Training-Log-Form.pdf

Appendix M – CJIS Supplement Guidance

See CSP – Appendix J at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

Appendix N – Agency Privacy Requirement NJC

https://www.fbi.gov/services/cjis/compact-council/guiding-principles-agency-privacy-requirements-for-noncriminal-justice-applicants

Appendix O – NCJ Applicant Privacy Rights

https://www.fbi.gov/services/cjis/compact-council/guiding-principles-noncriminal-justice-applicants-privacy-rights

Appendix P – NCJ Applicant Privacy Act Statement

https://www.fbi.gov/services/cjis/compact-council/privacy-act-statement

Appendix Q – ACIC Training Policy

http://www.acic.org/Websites/acic/images/pdfs/Training_Policy2015.pdf

Index