Arkansas Crime Information Center

# ACIC
# Duties and Responsibilities of the Terminal Agency Coordinator (TAC Officer)

Revision
November 29, 2017

Arkansas Crime Information Center
322 South Main Street
Little Rock, AR 72201
(501) 682-2222

***CONTENTS:***



***DEFINITION:***

A Terminal Agency Coordinator (TAC) is the vital communication link between your Terminal Site Agency and ACIC. By properly performing their duties they will ensure that your agency will be in compliance with ACIC/NCIC Policies, Procedures, Rules and Regulations. This will ensure the following:

1. Quality Records
    a. Timely
    b. Accuracy
    c. Supplemental Information
    d. Second party checks
    e. Validations
2. Satisfactory Audit Results
3. Quality Documentation for Liability Purposes
4. Coordinating Training
    a. Basic or Advance Certification
    b. CJIS Security Certification

Distribution of all ACIC documentation, communications and material to all agency personnel including briefing the Chief Official when appropriate. (*ACIC System Regulation: Appendix A*)
Notify ACIC of change in the status of personnel.

***PURPOSE:***

The Purpose of this Guide is to provide the TAC with the information they will require to properly perform and be successful in this position. Also, to give you the Terminal Site Agency the requirements and guidelines that are required for the TAC.

**A) Naming a Terminal Agency Coordinator:**

ACIC System Regulations requires each agency to designate a Terminal Agency Coordinator. (ACIC System Regulations, Section 10 Operators and Record Personnel (a)). The Head of an Agency has the sole authority to name or change the Terminal Agency Coordinator at his/her discretion. The TAC should be someone in supervisory status that is ACIC certified. (ACIC System Regulations) Section 9. Application, (a) Terminal Agency Coordinators This will give the TAC a better understanding of the requirements expected of an ACIC terminal operator. To "assign" or "change" the TAC, the Agency Head simply completes a Designation of T.A.C Form. This form is available on the ACIC Website ACIC.org or on the CJIS Launch Pad under CJIS Training Designation of T.A.C Form. Please complete the form in its entirety and fax to 501-682-7444. When designating or changing a TAC please contact your local ACIC Field Agent to advise him/her of the change. The Agency Head has the option of changing the TAC at any time by submitting a new form.

**Please note:**
**The TAC should immediately be changed when the current TAC is reassigned or leaves employment with the agency. ACIC should be notified immediately.**

**B) ACIC Conference and User Group Meeting:**

ACIC will host a User's Conference on a yearly basis. The conference is an important responsibility of the TAC. It is necessary to provide the Agency and the Users with information about important system changes, enhancements, legislation, and current best practice.

Conferences are held in central areas and every effort is made to keep costs to a minimum to help encourage attendance. Ideally, the TAC and the Agency Head should both attend the conference as topics are often presented that require decision-making by the agency's top administrator. Should the Agency Head not be able to attend, the TAC must ensure that all information is provided throughout his/her agency.

**It is expected that the TAC will attend the conference.** However, should the TAC not be able to attend, a representative from the Terminal Site Agency should attend in their stead.

Information and Registration for the yearly conference can be found on the ACIC website under **Training and Events**. ACIC Conference

Occasionally, ACIC will have a **User Group Meeting** to address a specific need. You will be provided with the time and place of these meetings in advance.
**It is expected that the TAC or his/her representative will attend.**

**These meetings should not be considered optional by the agency**.
Attendance is expected to ensure that your ACIC site has the latest information to provide your dispatchers, officers and administrative personnel. All current information available from ACIC/NCIC/NLETS will be provided during these meetings.

**C. User Information Update:**

ACIC works diligently to ensure we provide information to the TAC and Users in a timely manner through the following:

1. Terminal Messages
2. Daily Messenger "Tips of the Day"
3. CJIS Launch Pad - Launch Pad News, CJIS Documents, CJIS Training, CJIS Manuals, and Information Section
4. Monthly System Update Newsletter CJIS Documents System Update Publications (Sign in with CSN# and Password)
5. ACIC "Beginners Guide to ACIC" – CJIS Training
6. Training, Field Agents and Network Control

These are just a few examples of how ACIC works to ensure that your agency is not caught unaware of a system change that could potentially impact your operation.

Encourage your Users to notify the TAC of all System Updates/Training messages form ACIC Network Control. **Require that each of your Users read the System Update Newsletter (CJIS Documents). This will facilitate dissemination of information in a more timely and accurate manner.**

**D) System Security Assurance:**

According to the ACIC System Regulations, on-site security inspections will be conducted on all interface agencies. Section 4. Security (b) Security Checks
The TAC should work in conjunction with the Local Agency Security Officer (LASO) to ensure security of ACIC equipment and the information obtained from the ACIC System.

System Security includes but is not limited to the following:

1. Ensure that unauthorized persons are not allowed in the area of your ACIC workstation or other ACIC equipment
2. Ensure that departmental personnel do not attempt to make changes to the ACIC equipment (Hardware or Software)
3. Disposal of all ACIC documentation is done by burning or shredding (ACIC System Regulations) Section 4. Security (d) Disposal of Documents

4. Instruct all personnel on the proper dissemination of ACIC information
5. Contact ACIC personnel if there is a request for information and the validity or authority of that individual is in question
6. Educate Users in Password Security (See Section IX Passwords)
7. Notify your supervisor and your local ACIC Field Agent of any suspected security violations
8. Any changes, additions, or removals to the agency's network will require an updated **network diagram** (CJIS Security Policy).
9. Read and be familiar with the CJIS Security Policy.
10. Ensure that all agreements are up-to-date (examples: System Service Agreement, Holder of the Record Agreements, Management Control, etc.)
11. Review all of the department's internal policies related to ACIC (examples: Warrant Entry Policy, Missing Person Entry Policy, Audit Policy, Dissemination Policy, Vehicle Entry Policy, Training Policy, Validation Policy, Media Protection Policy, etc.).

**E) Coordinate Training of Operators and Documentation:**

All individuals operating an ACIC access device, including mobile devices, or with indirect access to criminal justice information (i.e. ACIC printouts or electronically stored data) must be trained. Training is necessary for the proper and effective use of the State and National Computer Systems. Required training is defined in the ACIC Training Policy, as approved by the ACIC Supervisory Board. ACIC Training Policy Please also reference the ACIC System Regulations Section 11. Training. When a new User is hired or assigned to an ACIC workstation the following procedure **must** be followed:

**i. Users with Direct Access**

1. A fingerprint based background check must be done with the FBI. (Blue Applicant Card is forwarded to Arkansas State Police Fingerprint Division) (Please reference Fingerprinting & Reporting Requirements for more information)
2. A background check must be done by utilizing ACIC/NCIC criminal history files. If the applicant has a **felony** record, they cannot have access to the ACIC system. (ACIC System Regulations, Section 10. Operators and Records Personnel, (d) Security Clearances) (This includes **sealed felony records**.) Please use the Purpose Code "J" for this transaction. (Reference Criminal History Purpose Codes)
3. Email or fax a copy of the Training Request Form to ACIC Training Division to allow password access by the new User. *(The email address and fax number is*

*located on the form.) (Note: New users are granted access for on the job training with a certified operator only*). **Please ensure that this form is signed by the agency's Chief Official or the TAC.** The form **must be completed in its entirety** or it will prompt a call from ACIC. An incomplete form will delay the user from gaining access to the system.

4. The TAC shall provide all new users with the **Beginner's Guide to ACIC**. New users shall complete the **Beginner's Guide to ACIC** before attending the ACIC Basic class.

5. New Users **must be trained and certified** within 90 days of employment. The ACIC Training Schedule can be accessed in three places: CJIS Launch Pad under CJIS Training in the ACIC Training Schedules folder , the Messenger Help Files under Training and the ACIC website under Training and Events. You must sign in with your username and password to access these files. (If using tokens see section X. Passwords)

6. There is a **mandatory** waiting period of **30 days** between completion of a Basic Operators class and the Advanced Operators class. This gives the user a sufficient amount of time to ensure successful completion of the advanced courseware.

7. All training class attendees must be in possession of proper departmental identification and a current driver's license to be admitted into the class.

8. **Notify ACIC as soon as possible if it becomes necessary to cancel a scheduled training session. This will allow other agencies access to the training class.**

9. Agencies are required to keep a training file on each User containing copies of certificates. This should be kept in their personnel file or in a separate training file. An ACIC auditor/agent may ask to inspect these records CJIS Security Policy 5.2.2 Security Training Records.

10. ACIC/FBI requires that all Users be recertified every **two (2) years**. This can be accomplished by logging into the nexTEST System and taking the Basic Certification Exam or the Advanced Recertification Exam. Once a User has been expired for a period of **one (1) year,** the nexTEST System will not allow them to retest. Therefore, they will have to attend an ACIC Basic class to begin the certification process again.

11. As the TAC, you will have access to the **Certification Expiration Report** in the nexTEST System. This report will allow you to check the "status" of all Users attached to your agency's ORI. You should review this report several times throughout the year to ensure that all of your Users are current and that you have notified ACIC of any changes in employee status. It is imperative that you notify ACIC when a User is no longer employed with your Agency. ACIC will then remove their access to ALL ACIC systems (Messenger, CENSOR, JusticeXchange, Metal Theft Investigative System, etc.)

To access the Certification Report take the following steps:

**a.** Access the Nextest NCIC Testing System Nextest Testing System

**b.** Sign on using the **Agency Login**, use your Username and Password

**c.** Choose the "Reports" Tab

**d.** Under Standard Reports, choose "**Certification Expiration Report**"

**e.** There is a dropdown box on the top of the form, scroll down to "Show All Users"

**f.** Next select "All Dates in Data Base" and Submit

**g.** Print and review the report for any updates required

**h.** Email ACIC Training Department with updates at nlenotifications@acic.arkansas.gov.

12. If you hire a previous ACIC User from another Agency, the TAC shall notify ACIC immediately to ensure their access and training records are transferred to your agency's ORI. Otherwise, their access may be disabled and their certification could expire.

Agencies with large numbers of Officers that are ACIC trained, such as agencies with Mobile Data Terminals (MDT's), should work with their Department Training Officer to ensure meeting the above standards.

**ii. Users with Indirect Access (ACIC printouts or electronically stored data)**

1. A fingerprint based background check must be done with the FBI. (Blue Applicant Card is forwarded to Arkansas State Police Fingerprint Division) (Please reference Fingerprinting & Reporting Requirements for more information)
2. A background check must be done by utilizing ACIC/NCIC criminal history files. If the applicant has a **felony** record, they cannot have access to the ACIC system. (ACIC System Regulations, Section 10. Operators and Records Personnel, (d) Security Clearances) (This includes **sealed felony records**.) Please use the Purpose Code "J" for this transaction. (Reference Criminal History Purpose Codes)
3. According to the user's job duties, the TAC will establish the CJIS Online account with the proper level of training/testing.
4. The TAC will periodically review the CJIS Online "Certification Expiration Report" to ensure all agency accounts (to include staff and contractors) are trained and current.

**Example of individuals who may need the CJIS Online Certification:**

- Janitors
- IT staff (agency or contractors)
- Maintenance Personnel

- Chief Officials or Officers who do not operate an ACIC workstation or mobile device.
- Court Clerks
- Judges
- Prosecutors

*Note: This list is not all-inclusive.*

5. ACIC/FBI requires that all Users be recertified every **two (2) years**.
6. Inactive users will remain on the agencies user roster.

## F) Validations:

Every agency that enters records into the ACIC/NCIC System must validate these records to ensure the completeness and accuracy of those records. While the TAC may or may not be the **Validation Officer** and perform these validations, they are to ensure that validations are completed as required by ACIC/NCIC Policy. The Validation Process is as follows:

**VALIDATION PROCESS**
On a monthly basis, ACIC will post a file containing records scheduled for validation for each originating agency (ORI). Validation is accomplished by:

1. Confirming that the agency has the required supporting documents for each active record. Records should be filed in a manner that allows verification and confirmation of hits within 10 minutes. Examples of supporting documents include warrants, protection orders, incident / offense reports, responses to ACIC queries such as criminal histories and wanted person responses, etc.
2. Comparing each record with its supporting documents and ensuring that all records are accurate and contain all available information.
3. Following up on all records by contacting the victim, complainant, prosecutor, court, and/or nonterminal agency to confirm the record's status.
4. Removing records that are no longer valid.
5. Correcting inaccurate records.
6. After the validation process has been completed the validation officer must use the BVAL form to batch validate or to manually validate each records with the VAL form. This confirms that the record has been reviewed, is accurate, complete and up-to-date.

Please refer to the **ACIC Validation Policy** and the **Validation Procedures Instructions** for more information. Remember that failure to follow the above steps could result in your agency's records being purged from the system. Accurate records are essential for the safety of your officers and reduces the risk of liability issues for your department.

**NO RECORDS SHOULD BE PURGED!!!!! Invalid records must be removed immediately.**

## G) Audits:

The Arkansas Crime Information Center is mandated by the National Crime Information Center to audit law enforcement agencies that utilize its system. The audit procedure not only serves to improve the existing criminal justice information system, but it should also detect problem areas that might hamper the system's operation. The ACIC audit involves four elements.

They are as follows:

1. **Compliance** – determines whether the agency is conforming to ACIC and NCIC policies and regulations.
2. **Efficiency** – determines whether the agency is managing and utilizing its records/filing system economically and efficiently allowing proper hit confirmation procedures.
3. **Data quality** – determines whether data integrity meets ACIC/NCIC minimum standards for accuracy thereby reducing potential agency liability.
4. **Effectiveness** – determines whether the desired results or benefits are being achieved.

Every law enforcement agency with records entered in ACIC/NCIC is audited a minimum of once every **three years**. Additional audits may be conducted, as needed if initial audit findings are not satisfactory. In all instances, the audit is used as an instrument for improving the Criminal Justice Information System, not for imposing penalties. Please refer to the Audit Policy and the How to Successfully Complete an Audit on the CJIS Launch Pad under CJIS Documents, Audits for more information.

If you require further assistance, you can contact your area ACIC Field Agent or the ACIC Validation Officer/Audit Coordinator, Kara Rice at Kara.Rice@acic.arkansas.gov or 501-682-7427.

## H) Criminal History Logging:

A record on all disseminations of criminal history information must be maintained. This record of each dissemination provides an audit trail that is required for correcting errors, for updating records that may be modified by judicial or administrative action, and for verifying access. A log of each criminal history requested through ACIC is electronically maintained in the ACIC system. Any agency retrieving criminal history information through ACIC and subsequently disseminating that information to another criminal justice agency outside the original receiving agency, is required to log this secondary dissemination. This manual log

will be in a format prescribed by ACIC and will be retained by the disseminating agency for a period of **one year**. ACIC System Regulations, Section 7. Criminal History Information, (e) Logging

Every Criminal History request (QH, QR & QWI) need not be logged. If the name of the requesting officer and ORI used in the inquiry match, then no logging is required. However, in any situation where you must use your ORI and the name of an officer who is employed by another agency, then complete information must be placed on the current log sheet and the log maintained for one year. One year is the minimum requirement, however please understand that this log is documentation that could potentially benefit you during an ACIC/NCIC audit.

**Examples of Proper Use of Dissemination Log**:

Example: If you are running a Criminal History for an outside agency, he/she should have their own ORI for their agency. Best practice is to run the transaction with his/her ORI and name, and then no manual dissemination log entry will be required.

Example: If you are running a transaction for an outside agency and the operator does not use that agency's ORI, then the transaction **must be logged** on the dissemination form.

Example: If your officer places a criminal history printout in a case file, which is subsequently given to the prosecuting attorney, this dissemination must be logged.

Each ACIC Terminal Site Agency is required by ACIC/NCIC policy to maintain a Criminal History Secondary Dissemination Log. **There are no exception to this policy.** If you do not currently have a log, please copy the above Criminal History Secondary Dissemination Log and train all Users on the proper use and requirement.

**Criminal History background checks for local businesses are prohibited. Please see attached document on page**….

## l) Passwords:

Agencies shall follow the secure password attributes, below, to authenticate an individual's unique ID. Passwords shall conform to the standards as listed in the CJIS Security Policy 5.6.2.1.1 Password:

1. Be a minimum length of eight (8) characters on all systems
2. Not be a dictionary word or proper name

3. Not be the same as the User ID
4. Expire within a maximum of 90 calendar days
5. Not be identical to the previous ten (10) passwords
6. Not be transmitted in the clear outside the secure location
7. Not be displayed when entered

**The above CJIS Policy is the minimum standard, however ACIC follows the following standard:**

1. Robust password structure is 8-15 characters, one alpha, one numeric, one capitol letter and a special character (#, &, *, $ etc...)
2. Not a word commonly found in the dictionary or proper name
3. Expires every 90 days
4. Not be identical to the previous ten (10) passwords
5. Not be transmitted, shared or displayed
6. A user's initial password will be assigned by ACIC. The system will require the user to create a **robust password**.
7. If using the ACIC Two-Factor Authentication Token, users will have an assigned password that will never change. The password will be immediately followed by the six (6) digit number that is displayed on the token.

**Arkansas Statute Annotated 5-41-206**, states that Computer password disclosure can be classified as either a Class A misdemeanor; or a Class D felony. Further, **18 United States Code Section 1030** states that if a computer is used by or for the Government of the United States provision of a password shall be subject to a fine under this title or imprisonment for not more than ten (10) years, or both. Please educate your Users in the importance of Password security.

# Contact Information

## NETWORK CONTROL (24 hours)

local 501-682-7415
Toll-free 800-482-5866
email: ACICHelp@acic.arkansas.gov

## Operations Division Administrator

Rick Stallings, Field Services Manager
Rick.Stallings@acic.arkansas.gov
(501) 682-7409or (501) 412-5077

## Operations Manager

Karen Burgess
Karen.Burgess@acic.arkansas.gov
(501) 682-7411 or (501) 231-2310

## Operations Field Services Manager

Vacant, Field Services Manager
@acic.arkansas.gov
(501) 682-

## Training Manager

Benny Battles, Training Manager
Benny.Battles@acic.arkansas.gov
(501) 682-7413

## Field Agents

Rhonda Ratterree, Southeast Arkansas
Rhonda.Ratterree@acic.arkansas.gov
(870) 454-7339

Kim Freeman, West Central Arkansas
Kimberlee.Freeman@acic.arkansas.gov
(501) 412-7322

Sunni Douglas, Southwest Arkansas
Sunni.Douglas@acic.arkansas.gov
(501) 412-6910

Sarah Cole, Northeast Arkansas
Sarah.Cole@acic.arkansas.gov
(870) 219-2983

Tiffanie Ward, Noncriminal Justice Auditor & Criminal History Auditor
Tiffanie.Ward@acic.arkansas.gov
(501)

Keith Weaver, Central and East Central Arkansas
Keith.Weaver@acic.arkansas.gov
(501) 454-7413

Zachary Osborne, Central and North Central Arkansas
Zachary.Osborne@acic.arkansas.gov
(501) 412-1996

Marc Arnold, Northwest Arkansas
Marc.Arnold@acic.arkansas.gov
(479) 621-3714

Michele Kulesa, VINE/JusticeXchange Coordinator
Michele.Kulesa@acic.arkansas.gov
(501) 682-9490

## Training Coordinator

Jennifer Tomlin, Training Coordinator
Jennifer.Tomlin@acic.arkansas.gov
(501) 682-7410

## Validation/Audit Coordinator

Kara Rice
Kara.Rice@acic.arkansas.gov
(501) 682-7427

# Designation
# Of
# Terminal Agency Coordinator (TAC)

**I, _____ do hereby designate, _____ to serve as the**

Chief Official — Rank or Title and Name

**Terminal Agency Coordinator (TAC) for the _____ department.**

Agency and ORI

**I understand that a TAC is expected to be the primary liaison between my Department and ACIC (Arkansas Crime Information Center). They are to actively represent my Department on matters relating to ACIC. They are to be familiar with the record system and communication needs of my Department. They are responsible for receiving information from ACIC and appropriately handling or disseminating the information within my Department. The designated TAC will keep ACIC informed on our training needs and other matters relating to the use of the *ACIC/NCIC/NLETS system.**

**I further agree to submit a new Designation form to ACIC at any time there is a change in the above named TAC.**

**Signature:** _____ **Date:** _____

Chief Official

**Signature:** _____ **Date:** _____

Designated TAC

**Contact Information for Designated TAC**

| **Email:** | **Phone:** |
|---|---|
| | |

**Please Mail or Fax Completed Form to:**

**Arkansas Crime Information Center**
**322 South Main Street, Suite 615**
**Little Rock, AR 72201**
**FAX: 501-682-7444**

*ACIC (Arkansas Crime Information Center)

*NCIC (National Crime Information Center)

*NLETS (National Law Enforcement Telecommunication System)

**Updated: 9/9/2014**

# ARKANSAS CRIME INFORMATION CENTER
# SYSTEM REGULATIONS

---

ADOPTED IN ACCORDANCE WITH THE
ADMINISTRATIVE PROCEDURE ACT

---

ARKANSAS CRIME INFORMATION CENTER
322 S. MAIN STREET, STE. 615
LITTLE ROCK, ARKANSAS 72201
501-682-2222

**Section 1. Authority.**

(a) **Scope.** These regulations apply to all criminal justice agencies and officials in Arkansas. Authority for these regulations that govern the operation and use of the Arkansas Crime Information Center (ACIC) system is found in A.C.A. §§ 12-12-203 (a)(5) and 12-12-203(b).

(b) **System Authorization.** The ACIC system was established by Act 286 of 1971, as amended, and codified in A.C.A. §§ 12-12-201 --12-12-214 and 12-12-1001 - 12-12-1015.

(c) **Administration.** ACIC is administered by a Director and a 14-member Supervisory Board. Membership of the Board is specified in A.C.A. § 12-12-202. This board appoints the ACIC Director and establishes the general policies and regulations governing the operation of the ACIC system.

(d) **Control Terminal Agency.** The National Crime Information Center (NCIC) and the National Law Enforcement Telecommunications System (NLETS) both require that each state designate a criminal justice agency as Control Terminal Agency (CTA) for their services. A.C.A. § 12-12-208 designates ACIC as the control agency in Arkansas for NCIC and NLETS.

**Section 2. Definitions.**

(a) **"Administration of criminal justice"** means performing functions of investigation, apprehension, detention, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice also includes criminal identification activities and the collection, maintenance, and dissemination of criminal justice information.

(b) **"Access device"** means a computer terminal, microcomputer workstation, mobile data device or other electronic equipment used to communicate with the ACIC computer system.

(c) **"Criminal history 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, informations, 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.

(d) **"Criminal justice agency"** means a government agency, or any subunit thereof, which is authorized by law to perform the administration of criminal justice, and which allocates more than one-half its annual budget to the administration of criminal justice.

(e) **"Criminal justice official"** means an employee, sworn or unsworn, of a criminal justice agency, performing the administration of criminal justice.

(f) **"Criminal justice purpose"** means a use for the administration of criminal justice.

(g) **"Disposition"** means information describing the outcome of any criminal charges, including acquittals, dismissals, probations, guilty pleas, nolle prosequi, nolo contendere pleas, findings of guilt, first offender programs, pardons, commuted sentences, mistrials in which the defendant is discharged, executive clemencies, paroles, releases from correctional supervision, or deaths.

(h) **"Governmental Dispatch Center"** means a non-criminal justice agency established and authorized by act of local government to provide communications support services to agencies of local government, including criminal justice agencies (A.C.A. §§ 12-10-301 to 12-10-323).

(i) **"Interface agency"** means an agency approved to be on the ACIC network with direct access to the ACIC system by computer terminal, microcomputer workstation, mobile data device or other electronic equipment.

**Section 3. Access and Use of Information.**

(a) **Access Authority.** Agencies and officials receiving information directly from the ACIC, NCIC and NLETS systems are limited to those that have been assigned an Originating Agency Identifier (ORI) number by the FBI. The ACIC Supervisory Board may also allow other agencies or officials access to information from state-controlled databases, when authorized by Arkansas law.

(b) **Use of Information.**. Information from the ACIC system shall only be used by criminal justice officials, acting in their official capacities, for criminal justice purposes. Any other non-criminal justice uses must be authorized by law, under procedures approved by the ACIC Supervisory Board, and may include the release of information to the public on wanted persons, missing persons, stolen property, hazardous materials, and road and weather conditions.

(c) **Availability of ACIC Services.** Interface agencies shall staff and operate at least one access device on a 24-hour-a-day, 7-day-a-week basis. Any exception must be specifically approved by the ACIC Director. Interface agencies shall provide assistance to other criminal justice agencies not equipped with an ACIC access device, to include record inquiries, message transmittals, and record entries or deletions.

(d) **Free-text Messages.** All free-text messages transmitted in-state over ACIC, as well as out-of-state over NLETS, shall be connected with official criminal justice responsibilities, and shall not include recruitment of personnel, non-criminal justice announcements, greetings or any other matters outside of official business.

(e) **Misuse of Information.** Misuse of information from the ACIC system is a misdemeanor or felony depending on the circumstances, as defined in A.C.A. §§ 12-12-212 and 12-12-1002(b).

(f) **Vehicle Information.** Pursuant to Act 1830 of 2001, Section 6(c), ACIC may provide vehicle information to towing and storage firms for a fee of ten dollars ($10.00) per record check.

**Section 4. Security.**

(a) **Facilities.** ACIC access devices shall be placed in areas with adequate physical security that will (1) prevent access by the public or other non-official personnel; (2) prevent access by unauthorized agency personnel: and (3) allow access to a minimum number of authorized agency personnel. Internal procedures shall be implemented that will protect not only access devices, but also

technical documents and any records associated with entries in the state and national systems. Identification shall be required before admitting equipment maintenance personnel or other officials from outside the agency.

(b) **Security Checks**. ACIC will conduct periodic on-site security inspections in all interface agencies to ensure compliance with the ACIC System Service Agreement, as well as ACIC, NCIC and NLETS security policies. Agencies will permit the inspector, after proper identification, to conduct appropriate review of all hardware, software, communications interfaces and operating procedures relating to the ACIC, NCIC and NLETS systems. Results of inspections will be reported to departmental officials. Security violations that remain uncorrected will be reported to the ACIC Supervisory Board.

(c) **Technical Security**. Interface agencies will be required to implement and/or comply with special technical security standards designed to prevent unauthorized access to information.

(d) **Disposal of Documents**. When printouts, listings or other official records from the ACIC system are disposed of, it must be done by shredding, burning or other appropriate methods that will prevent any subsequent access by unauthorized persons or for unauthorized purposes.

**Section 5 Completeness and Accuracy**.

(a) **Responsibility**. Agencies that enter records, or cause records to be entered into ACIC and NCIC, are responsible for their accuracy, timeliness, and completeness.

(b) **Entry of Records**. Agencies should enter into ACIC, and into NCIC when appropriate, information on wanted persons, missing persons, and stolen property, as soon as the minimum data elements required for entry become available. The FBI considers the entry of a record within 72 hours of origin to be timely. After entry, the FBI requires missing person records to be updated within 60 days with any additional information that may have been obtained. There is no required waiting period before entering any missing persons, and Arkansas law (A.C.A. § 12-12-205) requires the immediate entry of missing persons under the age of 18. Agencies must have procedures in place to verify the accuracy of all information entered into ACIC and NCIC, with such procedures to include a review or double-checking by a second-party immediately after the record is entered.

(C) **Supporting Records**. All entries in ACIC and NCIC must be substantiated by official documentation, including a warrant for entries in warrant files, a theft report for entries in stolen property files, and an incident report for other record entries. Copies of these supporting documents, whether in manual or automated form, must be on hand to support all entries and must be accessible within 10 minutes for hit confirmation purposes. This backup documentation shall be maintained, readily accessible, as long as the record entries are in the state and/or national information systems. Any entries lacking such backup documentation must be removed by the entering agency.

(d) **Extraditions and Distance Limitations**. For entries in the NCIC wanted persons file, a determination must be made, to the maximum extent possible, as to whether extradition will be authorized if the individual be located in another state. If distance limitations are to be placed on extradition of the individual, this information must be included in the entry. NCIC permits the entry of non-extraditable felony warrants for the purpose of officer safety, but such entries must contain the code NOEX in the miscellaneous field to indicate no extradition. Within Arkansas, if there are limits on the distance an agency will go to get an individual, this limitation must also be included in the entry.

(e) **Monitoring**. ACIC Network Control will continuously monitor record entries and system use to ensure that standards and rules are being met.

(f) **Record Purge**. To help maintain file integrity, out-dated records in the ACIC files are periodically purged on a schedule similar to NCIC. Each agency will be provided with a listing of its records that were removed. These records may be re-entered if the agency so desires.

(g) **Validations**. All agencies with entries in ACIC and NCIC are required to participate in a record validation program. Validation is necessary to ensure record accuracy and includes the following steps: (1) agencies with entries will be notified of certain records in ACIC and NCIC that are to be validated; (2) all records identified must be reviewed and compared with case file documents upon which the entries were based; (3) the current status is determined by checking for changes in extradition limits, by determining from owners of stolen property if recoveries have been made, by verifying with the courts that arrest warrants are still active and have not been recalled, and by determining that persons reported missing have not returned; (4) record entries that are no longer current must be corrected or removed from ACIC or NCIC by the entering agency; and (5) a validation form is signed to officially acknowledge that all records identified have been reviewed, are complete and correct, and that all non-current records have been deleted. Failure to comply with validation timetables and procedures will result in the removal of specified records from the ACIC or NCIC files, as well as other potential sanctions approved by the ACIC Supervisory Board.

(h) **Audits**. To ensure the completeness and accuracy of records in the state and national information systems, as well as the security of both the data and access devices, agencies will be audited at least every three years. The primary purpose of these audits will be to assist departments in identifying and correcting problems in record management and information security, thereby reducing the potential for liability. Audits will consist of an examination and review of (1) pre-audit questionnaires, validations, and training compliance; (2) system entries, backup documentation, and filing procedures; (3) compliance with applicable laws and regulations; and (4) compliance with security requirements. A written report of the audit, with any findings or recommendations, will be provided to the agency. Failure of the agency to take corrective action as suggested in the audit report may result in sanctions or other actions approved by the ACIC Supervisory Board.

**Section 6. Hit Procedures**.

(a) **Record Hits**. A "hit" is a positive response to an ACIC and/or NCIC inquiry. A hit is not in itself probable cause to arrest or seize property. A hit provides dates and information, which must be added to other facts, in determining probable cause and legal

justification for an arrest or seizure decision. All printouts relating to a hit should be retained by the requesting agency to document any probable cause actions.

(b) **Confirmation**. Upon receiving a hit, and prior to arresting or detaining a person, or seizing property, the inquiring agency must contact the entering agency to confirm the hit, preferably via the hit confirmation message procedure. Confirming means to determine (1) that the person or property inquired upon is identical to that shown in the record; (2) that the record is current and still valid; and (3) that extradition of a wanted person, the return of a missing person, or the return of stolen property to its rightful owner will be undertaken. When an inquiring agency receives a positive response to an inquiry and the whereabouts of the person or property inquired upon is not known, the hit(s) should not be confirmed. However, if the code NOAH (Notify ORI of All Hits) is in the MIS of the record, the ORI of the record should be notified and furnished details concerning the inquiry.

(c) **Response**. The originating agency (ORI) has the duty to promptly respond with confirming details upon receipt of a hit confirmation request. The ORI of the record must, within ten (10) minutes, furnish a positive or negative confirmation, or a notice via the hit confirmation message that a specified amount of additional time is necessary to provide such confirmation. A requesting agency that does not receive a response within ten minutes should generate a second request. If, within ten minutes after the second request, the agency again fails to receive a response from the ORI, the agency will generate a third message to the ORI. These requests will be monitored by ACIC and appropriate action will be taken to obtain a response and ensure compliance with system standards.

(d) **Locate**. The locating agency that receives a hit will place a "locate" on a record immediately after receiving confirmation that it is a valid hit. An exception would be when a wanted person record contains an extradition limitation in the MIS and the agency finding the person is outside the geographic area of extradition indicated. These records need not be confirmed and the record should not be "located". However, if the code NOAH (Notify ORI of All Hits) is in the MIS of the record, the ORI of the record is to be notified and furnished details concerning the inquiry.

(e) **Clear**. It is the responsibility of the entering agency to immediately "clear" a record after receiving notification of recovery or apprehension.

**Section 7. Criminal History Information.**

(a) **Responsibilities**. ACIC is authorized to administer the state computerized criminal history file, in accordance with A.C.A. §12-12-207 and §§ 12-12-1001-- 12-12-1015. The Arkansas State Police administers the state Identification Bureau where arrest fingerprint records are maintained.

(b) **Fingerprinting**. Law enforcement agencies arresting persons for offenses specified in A.C.A. § 12-12-1006, are required to fingerprint those persons at the time of arrest and to submit the prints to the state Identification Bureau within 48 hours.

(C) **Disposition Reporting**. Arkansas criminal justice agencies are required to report dispositions of criminal charges in accordance with A.C.A. § 12-12-1007.

(d) **Interstate Records**. Criminal history information may be retrieved through ACIC from the FBI, as well as directly from other states. Criminal history records obtained through the FBI Interstate Identification Index (III), and from other states through NLETS, are restricted to criminal justice use and may not be accessed for licensing or employment purposes, except criminal justice employment using purpose code "J", or other purposes specifically authorized by law.

(e) **Logging**. A record on all disseminations of criminal history information must be maintained. This record of each dissemination provides an audit trail that is required for correcting errors, for updating records that may be modified by judicial or administrative action, and for verifying access. A log of each criminal history requested through ACIC is electronically maintained in the ACIC system. Any agency retrieving criminal history information through ACIC and subsequently disseminating that information to another criminal justice agency outside the original receiving agency, is required to log this secondary dissemination. This manual log will be in a format prescribed by ACIC and will be retained by the disseminating agency for a period of one year.

(f) **Right of Challenge**. An individual has a right to see and challenge the contents of his or her criminal history record in ACIC, under controlled and reasonable administrative procedures, in accordance with A.C.A. § 12-12-1013. Requests should be addressed to the Administrator of the ACIC Criminal History Division.

**Section 8. Investigations, Violations and Appeals.**

(a) **System Control**. Although individual agencies retain certain responsibilities for their own records, overall system discipline and adherence to standards is required. Under Arkansas law, ACIC is authorized to control system use, enforce standards, and ensure that all users follow procedures.

(b) **Authority of Agents**. ACIC Information Agents are authorized by A.C.A. § 12-12-210. These agents provide technical assistance, system auditing and training to criminal justice agencies and officials. In addition, these agents may initiate investigations into the use or misuse of information from the ACIC, NCIC, or NLETS systems; may take statements, interview or otherwise compile information; may order the suspension of direct access pending correction of detected problems; and may develop written reports to departmental officials, to the ACIC Director, or to a prosecuting attorney when appropriate.

(c) **Violations**. When a violation of these regulations has been committed, or appears to have been committed: (1) an investigation will be initiated to determine the nature and extent of the alleged violation; (2) the chief official of the agency, or ranking officer in charge at the time, will be contacted and given an opportunity to correct or explain the alleged violation, unless the violation requires immediate action; and (3) appropriate sanctions will be imposed if a violation has been substantiated and remains uncorrected.

(d) **Sanctions**. An unsatisfactory resolution of a violation may result in one or more of the following: (1) removal of certain records from the state and national systems; (2) suspension of ACIC service to an agency on a temporary basis, until corrective

action is taken to the satisfaction of ACIC; (3) revocation of the authority of specific individuals to operate an ACIC access device; (4) termination of ACIC service to an agency on a permanent basis; (5) prosecution of an individual or individuals. Under A.C.A. § 12-12-212 and § 12-12-1002, unauthorized use of ACIC is a felony.

(e) **Appeal Procedure**. Any recommendation or findings by an ACIC Information Agent may be appealed to the ACIC Director. Any action by the ACIC Director may be appealed to the ACIC Supervisory Board. An administrative appeal may be requested by written notice to the ACIC Director or Chairman of the ACIC Supervisory Board. Appeals to the Board will be considered at a special meeting or at the next regular meeting following receipt of the appeal request.

(f) **Notice of Investigations**. It shall be the duty of all agencies to advise ACIC of any allegations, investigations and/or disciplinary actions regarding misuse of the ACIC system or information therefrom.

**Section 9. Application, Equipment and Fees.**

(a) **Application Procedure**. The appropriate expansion of the ACIC network is determined by need, legal authority and cost effectiveness. New interface agencies may be added to the network only according to guidelines established by the ACIC Supervisory Board. Applications will be submitted in writing to the ACIC Director; an on-site inspection and evaluation will be conducted by ACIC personnel; and approval will be based on legal authority, scope of jurisdiction, proximity to existing interface agencies, communications capabilities, and other factors deemed appropriate by the ACIC Supervisory Board.

(d) **Equipment**. Access devices and related equipment directly connecting to the ACIC computer system will be provided by ACIC, or specifically approved by ACIC. Any changes or relocation of such equipment must be approved in advance by ACIC. The interface agency will be responsible for any damage to the access equipment caused by the negligence of its personnel, or for any other damage which is, or reasonably should be, covered by local departmental insurance.

(c) **Fees**. Services and equipment to be provided by ACIC, along with any fees to be paid by interface agencies, will be approved by the ACIC Supervisory Board.

**Section 10. Operators and Record Personnel.**

(a) **Terminal Agency Coordinators**. The chief official of each interface agency will designate a Terminal Agency Coordinator (TAC) to act as the primary contact person for that agency. The TAC should have completed ACIC training requirements and shall (1) serve as liaison between the interface agency and ACIC, actively participating in meetings and providing input on system functions; (2) receive documents and materials from ACIC and distribute them to all appropriate personnel, including briefing the chief official when appropriate; (3) inform ACIC on personnel matters, including the names of individuals attending ACIC training classes, changes in operator assignments, and changes in TAC designation; and (4) assist ACIC personnel in record audits, security checks, and other matters within the interface agency.

(b) **Local Agency Security Officers**. The chief official of each interface agency will designate a Local Agency Security Officer (LASO) to (1) act as the point of contact for information security matters; (2) receive basic and on-going security training from ACIC; (3) distribute security alerts to employees of the interface agency; (4) assist the ACIC Information Security Officer (ISO) with security awareness training; and (5) assist state and federal auditors with technical audits in the interface agency.

(c) **Assignment of Operators**. Operators are a critical link in any telecommunications system. The integrity, skill and knowledge of operators is vitally important to effective law enforcement communications. ACIC strongly endorses the principle that permanently assigned professional communications operators should be employed in all dispatch and communication centers.

(d) **Security Clearances**. Personnel assigned to operate ACIC access devices, including mobile devices, shall be identified on forms furnished by and returned to ACIC. These forms shall be signed by the chief official of the agency and will include a statement acknowledging that a state and national fingerprint-based background check has been conducted on each operator. To be eligible to operate an ACIC access device, or to receive information directly from the ACIC system, operators and other criminal justice personnel in both interface agencies and non-interface agencies shall not have entered a plea of guilty, been found guilty or convicted of a crime which is a felony. This requirement will be interpreted consistent with A.C.A. § 16-90-902.

(e) **Minimum Age**. The minimum authorized age for an individual operating an ACIC access device is 18.

(f) **Volunteer Operators**. Officially designated volunteer and auxiliary personnel may be used as access device operators, provided they meet the same requirements and training standards as regular operators. Interface agencies shall be responsible for all actions of these volunteer or auxiliary operators.

(g) **Citizenship**. Any person operating an ACIC access device must be a U.S. citizen or a legal alien specifically approved by ACIC.

**Section 11. Training.**

(a) **Operator Training**. All individuals operating an ACIC access device, including mobile devices, must be trained. Training is necessary for the proper and effective use of the state and national computer systems. Required training is defined in the ACIC Training Policy, as approved by the ACIC Supervisory Board.

(b) **Officer Training**. ACIC provides a general overview of the state and national computer systems to law enforcement officers during all basic classes at the Arkansas Law Enforcement Training Academy or other authorized basic training entities. ACIC will also provide training, upon request, for officers in any department. Such training will be tailored to what a street officer needs to know about the state and national computer systems.

(c) **Other Training**. ACIC periodically provides special orientation classes for criminal justice officials. These sessions emphasize general system capabilities, state and national policies, liability issues, and matters of administrative interest.

**Section 12. Agreements.**

(a) **System Service Agreements.**. The chief official of each interface agency is required to sign a System Service Agreement, and other agreements as appropriate, outlining their duties and responsibilities concerning ACIC, NCIC, and NLETS policies and procedures. Such agreements will be re-executed as required by the ACIC Supervisory Board.

(b) **Holder-of-the-Record Agreements**. A criminal justice agency that enters records into the ACIC or NCIC systems must ensure that any hits on its entries can be confirmed 24-hours-a-day, 7-days-a-week. An agency not continuously operational will execute a holder-of-the-record agreement with another agency that is continuously operational. Under such an agreement, the non-24-hour originating agency authorizes the 24-hour holder-of-the-record agency to enter, update and remove records, as well as confirm hits on the originator's records. The originator is responsible for immediately notifying the holder of any changes in the status of originator's records.

(c) **Management Control Agreements**. Access by non-criminal justice Governmental Dispatch Centers is allowed, provided an agreement has been executed giving management control to a criminal justice agency. Management control is defined as the authority to set and enforce (1) priorities; (2) standards for selection, supervision, and termination of personnel; and (3) policies governing operations, insofar as those policies apply to law enforcement communications and records.

(d) **Other Agreements**. The ACIC Supervisory Board may require the executive of other agreements to cover privatized criminal justice functions or other special situations.

**Section 13. Exemptions.**

Any exception to the requirements of these ACIC System Regulations must be specifically approved by the ACIC Director or ACIC Supervisory Board.

Appendix B

# ARKANSAS CRIME INFORMATION CENTER
# CRIMINAL HISTORY SECONDARY DISSEMINATION LOG

YOUR AGENCY: _____ YOUR ORI: _____ PAGE: _____

| Date | Time | Subject's Name, Race, Sex, and DOB OR Subject's SID Number or FBI Number | Name, Rank/Title of person whom the Record was given | Reason for Request (Be Specific) | Person Making Dissemination |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

All criminal histories obtained through ACIC, NCIC, and III **using your own ORI**, then given to another criminal justice agency must be logged. The Secondary Dissemination Log must be kept for a minimum of one (1) year.

Appendix C

# Criminal History

## Use and Dissemination Guidelines

The purpose of this document is to provide guidance to the ACIC user as to the proper use and dissemination of criminal history information. While every circumstance cannot be covered in this document, general guidelines and some specific examples will be covered in an effort to provide the user with the knowledge needed to access and use criminal history information.

### *What is Criminal History?*

"Criminal history 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, informations, 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. (Source: [1] Arkansas Crime Information Center, System Regulations)

The Arkansas Crime Information Center is the repository for criminal history in Arkansas. Arkansas criminal histories are forwarded to the FBI's Interstate Identification Index (III). The Interstate Identification serves as an index of criminal histories in the United States. One check of the III will result in a response indicating the state(s) that the subject of check has criminal history.

### *Types of Criminal History checks*

There are several types of criminal history checks. The two major categories are Criminal Justice and Civil.

### *Criminal Justice Criminal History Checks*

Criminal Justice criminal history checks can be performed by a "criminal justice official" for the "administration of criminal justice". Checks conducted through the ACIC automated system are for criminal justice purposes. These are name based checks. Name based checks are not as reliable or as through as fingerprint based checks. These checks can be performed on an ACIC workstation but only for specific purposes. Each criminal history transaction must include a purpose code indicating the purpose of the criminal history check. Following is a list of the acceptable criminal history purpose codes taken from the NCIC Operating Manual:

**Purpose Code A--Administrative File Maintenance**

*(This code is used only by ACIC and Arkansas State Police Identification Bureau.)* Purpose Code A is used by authorized participating state agencies to retrieve records for internal review. Purpose Code A responses cannot be disseminated for any other purpose. A QR for Purpose Code A allows a state to review CHRI, want, and sexual offender registry notifications that are in the III for that state.

**Purpose Code C--Criminal Justice**

(Purpose Code C is used for official duties in connection with the *administration of* criminal justice.) The following examples provide clarification of authorized uses of Purpose Code C in situations that are not part of a criminal justice investigation but are duties of the agency where a criminal record check is necessary to accomplish the agency's mission. These examples are not all encompassing.

1) Authorized uses of Purpose Code C in relation to the security of the criminal justice facility include:
   A) Vendors or contractors at the criminal justice agency who are not involved with the actual administration of criminal justice at the criminal justice agency, e.g., carpet cleaners, individuals responsible for maintaining vending machines, janitors, and cooks.
   B) Volunteers at a criminal justice agency who are not involved with the actual administration of criminal justice at the criminal justice agency, e.g., participants in community ride-along programs and volunteers at a confinement facility who are providing social or community services rather than rehabilitative services.
   C) Confinement facility visitors. D) Inmates of a confinement facility. E) Inmate mail (a prisoner's list of names and addresses of those wishing to correspond with the prisoner). The III may be used when there is reason to believe that criminal activity is occurring or has occurred.
   F) Participants of law enforcement-sponsored firearms training classes held at a public firing range that are handling firearms, and individuals attending firearms training events held at law enforcement facilities.

2) Purpose Code C is used by Governmental Social Service agencies with child protection responsibilities and the National Center for Missing and Exploited Children to access FBI criminal history record information under Section 151 of the Adam Walsh Child Protection and Safety Act of 2006 (Public Law 109-248). An NCIC Originating Agency Identifier (ORI) ending in the alpha character "F" has been established for Section 151 access.

**Purpose Code D--Domestic Violence and Stalking**

Purpose Code D is used when the III transaction is for use by officials of civil or criminal courts in domestic violence or stalking cases. Civil courts may be issued ORIs containing a D in the ninth position, at the discretion of the appropriate state CJIS Systems Officer (CSO) and the FBI's CJIS Division. ORIs ending in D are limited to QH and QR transactions for Purpose Code D.

**Purpose Code F--Weapons-Related Background Checks**

Purpose Code F is used by criminal justice agencies for the purposes of (a) issuing firearms-related permits and explosives permits pursuant to state law, regulation, or local ordinance; (b) returning firearms to their lawful owners; and (c) enforcing federal and state laws prohibiting certain persons with criminal records from possessing firearms in circumstances in which firearms have been pawned.

**Purpose Code H—Housing**

Purpose Code H is used when the III inquiry is made under the authority of the Housing Opportunity Extension Act of 1996. The use of this purpose code is limited to QH transactions. The FBI's CJIS Division may assign Public Housing Agencies ORIs containing the letter Q in the ninth position for use by authorized agencies.

**Purpose Code J--Criminal Justice Employment**

Purpose Code J is used when the III transaction involves 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. Such screening may include the use of III on friends, relatives, and associates of the employee or applicant, unless restricted or prohibited by state statute, state common law, or local ordinance. Criminal Justice Employment (Purpose Code J) has been separated from other Criminal Justice Purposes (Purpose Code C) due to the varying requirements of some state agencies participating in the III. Purpose Code J is used for initial background checks of agency personnel as well as the following: Noncriminal justice agencies that are involved with the administration of criminal justice on behalf of the criminal justice agency.

Vendors or contractors who are involved with the administration of criminal justice for the criminal justice agency, e.g., personnel involved with maintenance of computer systems, upgrading records systems, data entry clerks, etc.

Volunteers at the criminal justice agency who are involved with the administration of criminal justice for the criminal justice agency, e.g., volunteer dispatchers, volunteer data entry clerks, volunteers at a confinement facility who are providing inmate rehabilitation, etc.

## *Civil Criminal History Checks*

Various state and federal laws allow and/or require criminal history background checks. Civil checks are conducted through the Arkansas State Police Identification Bureau. Civil checks conducted through the ASP ID Bureau may consist of a check of only the Arkansas criminal history records or a check of both Arkansas criminal history records and national criminal history files maintained by the FBI. Civil criminal history checks conducted against the national criminal history files must be authorized by a state law that meets the requirements of Public Law 92-544.

Civil criminal history checks conducted against the Arkansas criminal history file must be authorized by law or by the consent of the subject of the check. These checks may be name based and can be conducted through the Arkansas State Police's Online Criminal Background Check System.


Arkansas Crime Information Center

# Audit Policy

Revision
June 1, 2018

Arkansas Crime Information Center
322 South Main Street
Little Rock, AR 72201
(501) 682-2222

# ***Criminal Justice Agencies***

The Arkansas Crime Information Center (ACIC) is mandated by the National Crime Information Center (NCIC) to audit law enforcement agencies that utilize its system. The audit procedure not only serves to improve the existing criminal justice information system, but it should also detect problem areas that might hamper the system's operation. The ACIC audit involves four elements. They are as follows:

A. Compliance – determines whether the agency is conforming to ACIC and NCIC policies and regulations.
B. Efficiency – determines whether the agency is managing and utilizing its records/filing system economically and efficiently allowing proper hit confirmation procedures.
C. Data quality – determines whether data integrity meets ACIC/NCIC minimum standards for accuracy thereby reducing potential agency liability.
D. Effectiveness – determines whether the desired results or benefits are being achieved.

Every law enforcement agency with direct access to ACIC/NCIC will be audited a minimum of once every three years. The site's level of access will determine the type of audit that will be conducted. Agencies that are full access sites will have a full records audit while agencies with limited access will have a site security audit. Additional audits may be conducted as needed if initial audit findings demand such action be taken. In all instances, the audit is to be used as an instrument for improving the criminal justice information system, not for imposing penalties.

***Audit Process***

The audit period begins January 1st of each year. All audit assigned during the period must be completed by September 1st allowing all re-audits to be completed and returned by December 1st.

The ACIC Audit Coordinator is responsible for overseeing the entire audit process. Questions or information about the audit may be addressed by the coordinator, however, scheduling changes and follow-up visitations or modifications are the responsibility of the auditor.

## *I. PREPARATION*

A. Forty-five days before an audit, the coordinator will send the agency a pre-audit packet to introduce the audit date, and include copies of ACIC's Audit Program, System Regulations Manual, Record Validation Policy, and Terminal Training Policy. A pre-audit questionnaire will also be included in the packet, which will be used for gathering data prior to the audit. It also serves the purpose of making agencies aware of policies and procedures that will be reviewed. The packet will also contain a list of criminal history transactions. The agency must review each criminal history transaction and list the reason the person was queried. The packet will be sent to the TAC (Terminal Agency Coordinator) and only the cover letter introducing the audit date will be sent to the administrator.
B. The agency's TAC or Records Coordinator should complete and return the pre-audit questionnaire, the criminal history transactions and any additional required documents to ACIC *no later than 20 days prior to the audit.*

Copies of the agency's most recent criminal history queries, training records, the pre-audit questionnaire, a sample printout of records in the system, and an audit fact sheet (which includes results from the most recent audit, purges due to poor validations, delayed hit responses, and Holder of Record agreements) will be reviewed in the audit.

## *II. AUDIT*

***The audit will have three phases: Data Quality Review, Policy and Procedure Review, and a Findings Conference.***

### *A. Data Quality Review*

1. This phase of the audit consists of reviewing a sample of the agency's ACIC/NCIC entries. This task will be done by pulling the physical files used for entry and reconciling them with the data file records. A maximum sample size of 25 records per file will be used. The files subject to audit will

include Wanted Person, Missing Person, Violent Person, Gang and Terrorist Organization, Protection Orders, Vehicles, Boats, and Parts.

a. Scoring of the records are as follows: each record is worth a total of 5 points with the exception of protection orders which are worth a total of 6 points per record due to the Brady Indicator.
    i. Example 1 – If a wanted person record is found to be invalid, 5 points will be deducted automatically for that record and will be shown as 1 invalid record. No other points can be deducted from that record.
    ii. Example 2 – If it is found that the agency neglected to include 5 AKAs in one record, 1 point will be deducted for that record and will be reflected as 1 incomplete record.
b. The point scores do not include second party check and validations. This is assessed in the Policy and Procedures Review.

2. Complainant contact on applicable records will be made by the auditor as part of the audit to verify proper validation procedures are being followed and the records are valid.

Discrepancies uncovered in the data records require immediate correction to reflect the information contained in the officer's report. Entries not supported by a physical file will be subject to immediate removal from the system. Errors found in this phase of the audit directly affect the review of policies and procedures phase of the audit.

### *B. Policies and Procedures Review*

1. This phase of the audit will commence with a structured and in depth review of several policies and procedures as described in the ACIC Regulations Manual and interface agreement as applicable. Four primary areas will be reviewed; the first of which is Administrative procedures. This includes review of proper validation, hit confirmation, packing the record, record removal, timely entry, and 2nd party review procedures as applicable to each agency under audit.

2. The next area to be reviewed will be Terminal Operator Training. Training records will be reviewed to ensure personnel are properly trained. Also, during this time, the agencies JusticeXchange user accounts will be reviewed to ensure security of that system.

3. Terminal Security is the next area that will be reviewed which includes policies on security, disposal of printouts, Internet access, background checks, and whether an agency can perform unauthorized transactions on the ACIC terminal.

4. The last area to be reviewed will be Criminal History procedures. This area is centered around reviewing an agency's policy on dissemination logging.

### *C. Findings Conference*

1. Upon completion of the data quality review phase, the auditor will conduct an exit interview with the agency's chief official and the TAC to discuss findings, possible problems and recommendations.

2. It is during this process that any discrepancies, misunderstandings or misconceptions between

the auditor and the agency are clarified to ensure the final written report reflects a true and accurate finding of the agency's policies, procedures and guidelines associated with records. Also at this time, based on the auditor's findings, appropriate action (modification or removal of records) should be taken by the agency.

## *III. AUDIT REPORT*

The auditor has thirty (30) days to submit a completed audit report to the ACIC Audit Coordinator for final review. Once the report is finalized, the audit report based on the auditor's findings will be forwarded to the chief official, auditor, and local agent. In addition, copies will be maintained by ACIC. The written assessment of the agency will include:

1. A description of any weaknesses found in the agency's internal control systems.
2. Notations about significant instances of non-compliance with ACIC/NCIC regulations, polices, or procedures found during or in connection with the audit.
3. Audit findings, recommendations for actions to improve problem areas, suggestions to improve operations and other pertinent information discussed with the agency official.
4. A description of noteworthy accomplishments, particularly when this information may benefit other agencies.
5. In essence, all information discussed during the exit interview should be included in the final audit report to ensure a fair and thorough outcome.

## *IV. SANCTIONS*

### *A. Record Quality*

1. As a result of the auditor's findings and recommendations made in the final audit report, ACIC may impose sanctions, based on the following guidelines:

a) Determine a percentage of error for each data file (i.e., wanted, missing, vehicle, etc.)
b) If the error rating is at or below 10%, no other action will be taken regarding the data files under audit.
c) If the error rating exceeds 10%, ACIC will notify the agency in writing of the errors via the audit report and re-audit the agency's bad file(s) within 90 days if the number of new and/or old records mandate it. The local ACIC agent will conduct the re-audit and is available to assist the agency in the correction process prior to the re-audit.
d) If at the time of re-audit, the agency's file(s) remain(s) above 10% rating, the chief official of the agency must appear before the ACIC Supervisory Board to present an outline of the steps that will be taken to meet the compliance standards. If the agency's chief official does not appear The ACIC Supervisory Board could take the following actions:
    1) Purge records in the questionable file(s), with the exception of the Missing Person file, Protection Order file and Violent Person file.
    2) Prohibit the agency's entry capabilities in that/those file(s) until compliance is achieved.

In order to be reinstated and regain the ability to enter records, the chief official of the agency must appear before ACIC Supervisory Board, outlining in detail the steps the agency has taken to meet compliance standards.

2. Any agency where sanctions are imposed will be subject to an audit the following year.

### *B. Policies and Procedures*

1. Consideration will also be given to policies in the four areas described in section II, A. These policies and procedures will be evaluated to determine compliance in this area of the audit.
2. If an agency is found out of compliance in any policy or procedure, a request for a "policy correction letter" will be made in the cover letter of the audit report. The letter must list the steps the agency will take or has taken to improve their procedures. The violations must be responded to *within thirty days* of the date on the audit report. Failure to comply with this request will result in the agency being reported to the Operations Sub-Committee of the ACIC Supervisory Board for a recommendation of action to be taken.
3. Agencies which have repeated areas of non-compliance from audit to audit and do not show any changes in their procedures to improve those areas will be subject to further audit procedures. Agencies may also be reported to Operations Sub-Committee of the ACIC Supervisory Board for a recommendation of action to be taken.

# ***Noncriminal Justice Agencies***

The Arkansas Crime Information Center is mandated by the National Crime Information Center to audit Arkansas noncriminal justice agencies that request Criminal History Record Information (CHRI).
Every noncriminal justice agency with a state statute which authorizes a fingerprint based background check, reviewed by the FBI and approved under Federal Public Law 92-544 will be audited once every three years. Additional audits may be conducted as needed if initial audit findings demand such action be taken.
The purpose of the ACIC audit is to help agencies identify problems and to improve their record systems, not to impose criticisms or penalties. This audit is meant to assist agencies in meeting the requirements of the CJIS Security Policy, Out Sourcing Standard, and Title 28, Code of Federal Regulations (CFR), Section 16.34 while improving efficiency and the security of CHRI helping to guard against situations that could create a liability risk for the agency.

This report is divided into the following six sections:

A. Use of CHRI

B. Dissemination of CHRI

C. Security of CHRI

D. Outsourcing

E. Reason Fingerprinted and Purpose Code Usage

F. Applicant Notification and Record Challenge

### *I. PREPARATION*

Thirty days before the audit, the Noncriminal Justice Agency Auditor will send the agency (Chief Official and the Noncriminal Justice Agency Coordinator [NAC]) a Pre-audit Questionnaire that is used to gather data prior to the audit. It also makes agencies aware of policies and procedures that will be reviewed. The agency's noncriminal justice agency coordinator or Records Coordinator should complete and return the pre-audit questionnaire and any additional required documents to ACIC *no later than 20 days prior to the audit.*

### *II. AUDIT*

***The audit will have three phases: Fingerprint and Criminal History Review, Policy and Procedure Review, and a Findings Conference.***

### *A. Fingerprint and Criminal History Review*

This phase of the audit consists of reviewing a sampling of the agency's fingerprint background checks to include the applications or supporting documentation. This task will ensure that the agency is completing the reason fingerprinted and the statute number field on the fingerprint cards. The auditor will review the application and supporting documents to ensure the agency has reason to perform a FBI fingerprint based background check. A maximum sample size of 25 identification records will be used per ORI.

Errors found in this phase of the audit directly affect the review of policies and procedures phase of the audit.

### *B. Policies and Procedures Review*

This phase of the audit will commence with a structured and in depth review of policies and procedures as described in the ACIC Systems Regulations, CJIS Security Policy, Public Law 92-544 approved state statute(s), Title 28, Code of Federal Regulations (CFR), Section 16.34, and Outsourcing Guide as applicable. The items that will be reviewed: User Agreements, Current NAC form, Dissemination Log, CJIS training records, Outsourcing Agreements, Application, Application Notification and Challenge, processed fingerprint cards, FBI Criminal History results, letters to applicants, and policies and procedures.

### *C. Findings Conference*

Upon completion of the Fingerprint and Criminal History Review and the Policies and Procedures Review phases, the auditor will conduct an exit interview with the agency's chief official and the NAC to discuss findings, possible problems and recommendations.

## *III. AUDIT REPORT*

The auditor has thirty (30) days to submit a completed audit report to the Field Services Manager for final review. Once the report is finalized, the audit report based on the auditor's findings will be forwarded to the chief official and local agent. In addition, copies will be maintained by ACIC. The written assessment of the agency will include:

1. A description of any weaknesses found in the agency's internal control systems.
2. Notations about significant instances of non-compliance with ACIC regulations, CJIS Security Policy, Out Sourcing Standard, and Title 28, Code of Federal Regulations (CFR), Section 16.34 procedures found during or in connection with the audit.
3. Audit findings, recommendations for actions to improve problem areas, suggestions to improve operations and other pertinent information discussed with the agency official.
4. A description of noteworthy accomplishments, particularly when this information may benefit other agencies.
5. In essence, all information discussed during the exit interview should be included in the final audit report to ensure a fair and thorough outcome.

## *IV. SANCTIONS*

### *Record Quality/Policies and Procedures*

As a result of the auditor's findings and recommendations made in the final audit report, ACIC may impose sanctions based on the following guidelines:

1. The agency must submit an action plan within 30 days describing the action taken to correct any issue found during the audit.
2. Once the initial action plan has been submitted, the ACIC auditor may request periodic updates on the status of the actions taken to correct the issues outlined in the final report.
3. ACIC will audit the agency the following year to address any noncompliance issues that were found during the audit.
4. Agencies that have not taken corrective action as outlined may be reported to the Operations Sub-Committee of the ACIC Supervisory Board for a recommendation of action to be taken.

Appendix E

## How to Successfully Complete an Audit

Most TACs tend to get over-anxious and upset when they get that dreaded summons to the Chief or Sheriff's office, only to discover that he has received notification of an upcoming ACIC audit. Most (if they are lucky) have already received notification themselves and can be prepared to confidently discuss the pending audit with their boss. At any rate, audits are a necessary evil and can greatly enhance one's appreciation for detail and accuracy. Further, they can be a very impressive confidence builder, not only in the TAC, but for the Chief or Sheriff as well, if his team is fully prepared and their records are in order. In short, if you are ready for an audit, it can be refreshing verification by the state that you are confident, professional and prepared. And if you are in panic mode, then it will reflect that maybe you have been less diligent than you should have been.

The purpose of this document is to help you by walking you through a successful audit and better prepare you to complete the task with ease and appear professional to your supervisors and state auditor staff.

First, don't panic. Your local ACIC Field Agent is at your disposal and available to assist you in getting ready for your audit. Of course, you shouldn't call them up the night before with impossible tasks or requests. But they are your lifeline and are there to assist you with any questions you have during the audit process.

Next, get over the term AUDIT. It is nothing more than a "visit" from ACIC personnel that you normally don't see. And they want to verify your records, as well as your manner of conducting business as it pertains to ACIC. And lastly, they are here to help you with any problems that you and your Field Agent haven't identified. They are essentially, a new assessor of your operations. And they don't come into the audit with any preconceived notions of your operations. They are there to identify problems and to recommend positive steps to improve your record systems, not to impose criticism or penalties. THEY WANT YOU TO SUCCEED.

Your audit process begins at least 45 days prior to the audit date with a notification to the TAC and Chief or Sheriff. The TAC should have received a pre-audit questionnaire. Completing and returning this form is vital to getting information to the auditor so that he/she can adequately evaluate your operation.

Also included with the pre-audit questionnaire is the random listing of Interstate Identification Index (III) transactions ran by your agency. You should begin immediately to verify this information, as it generally takes up to 45 days to track down each officer to verify the reason for running each transaction. The auditor will request WHY did each of these transactions take place? The Auditor may also verify that each transaction was requested by a member of your agency, and in the case of those outside your agency, whether the transaction is recorded on your dissemination log.

The day of your audit, greet your auditor, request and verify his/her identity by requesting ACIC identification. Take nothing for granted. This is an ACIC requirement and failure to properly secure the identity of those accessing your system, could result in sanctions against your agency. The Auditor will probably want to visit with your TAC and CEO informally and use this time to assess your overall preparedness and methodology. A whole lot of material can be covered here, both good and bad. You are setting the tone of the audit with this interview. Relax and learn from your Auditor what he/she is seeking. Ask questions here if there is something that you don't understand. This is your time to get tuned into the ground rules that will follow during the

audit. If you anticipate problems, explain it to the Auditor at this time. You may be needlessly worried about something that can be overcome here and ease your anxiety.

The Auditor will generally go over the pre-audit questionnaire (PAQ) with you at this time, verifying information contained therein. The answers you provide at that time will be vital to your successful completion of the audit. The Auditor is also assessing your understanding of ACIC regulations, policies and procedures during this time. At this point the Auditor will review the PAQ completed prior to their arrival to clarify questions and answers. This is the opportune time to ask questions you may have.

Next, the Auditor will usually verify some information that he/she has been provided by staff at ACIC headquarters. You will receive a printout of employees that have been trained and asked to verify whether they are still employed and mark those no longer employed by your agency with the initials "NLE" for no longer employed. This is to verify and validate our training records and JusticeXchange records.

You will be given a new System Service Agreement to be signed by your Chief or Sheriff. If this can be accomplished during the audit it is best. If not, it can be accomplished after the audit and mailed back to the ACIC Director. ACIC will mail your agency a copy for your files.

Next comes the records review. You will be asked to provide documentation of your records to verify that they are correct and complete. You may hesitate and ask. "Isn't that what Validation is for?" You are absolutely correct. If you have completed your monthly validations correctly and completely on a monthly basis, you are going to sail through this remarkably. Remember, this is only a random sampling of no more than 25 records in each category or all your records. The Auditor is looking for verification <u>independent agency paper file</u> of the existence of all information contained in the record, proper validation of the record, which includes contacting the originating party to verify the information contained therein), and "packing the record" in situations where additional information exists and could have been used as identifiers in most cases of the original records. You should treat this records review like each was a hit confirmation, verifying all the information within a 10-minute window.
This can be the most time consuming and tasking part of the audit.

Once this portion of the audit is complete, your Auditor may desire to conduct an exit interview with the Head of Agency as a courtesy to inform him/her of the agency's concerns from the audit. If successful, this is a good opportunity for the TAC to get a well deserved pat on the back. If unsuccessful, an opportunity for the Auditor to instruct the Agency Head in how the discrepancy can be corrected and avoided in the future as well as what to expect on the re-audit. This is usually a good time to explain the audit to the Head of Agency so that there are no misunderstandings upon receipt of the audit. The Auditor will state and explain any discrepancies and lay out an operational plan to overcome them upon re-audit.

Re-audits are conducted within 90 days by the Field Agent assigned to the agency. The agency is only re-audited in the area(s) where there was previously noted a more than 10% deviation (failure rate) in records. Should an agency fail to successfully complete a re-audit, the audit results will be taken before the Supervisory Board for review and possible sanctions up to and including revocation of system privileges.

The ACIC audit staff is available from beginning to end to assist your agency in your audit preparation. Our goal is to have a successful audit and we will work diligently with your department to reach this goal. Audits occur tri-annually.