Arkansas Crime Information Center

Audit Policy

Revision
May 4th, 2026

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. Both full access and limited access sites will have a CJIS IT 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 audits assigned during the period must be completed by September 30th allowing all re-audits to be completed and returned by December 31st.

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 letter to introduce the audit date, the ACIC auditor, and the User ID and Password that the TAC will need to log into the online auditing software. This letter will be sent to the TAC (Terminal Agency Coordinator). Included with the pre-audit letter is a list of criminal history transactions. The agency must review each criminal history transaction and list the reason the person was queried.
    a. The criminal history transaction review should be completed and kept on-site for the auditor to review at time of audit.
B. An additional letter introducing the audit date will be sent to the administrator.
C. Once your agency has been assigned an audit, the TAC will receive an email notification stating: *Your agency has been assigned a Pre-Audit Questionnaire/Audit. Please login to the CJIS Audit system to complete this audit.* Your User Name/Password for the CJIS Audit System is provided in the pre-audit letter.

The agency's TAC or Records Coordinator should complete the pre-audit within the online auditing software *within 30 days of it being assigned.* 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 within the audit software. Once the report is finalized, an email will be sent to the chief official and/or TAC advising that "*An audit has been reviewed for your agency. Please login to the CJIS Audit system to view this audit."* The acknowledgement of this audit report shall be submitted within 15 days of receiving the *review response notification*. In addition, copies will be maintained by ACIC. The 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, policies, 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 rating 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%, the ACIC audit software will notify the agency via email. A re-audit of the files with errors that exceed 10% will take place 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, an email notice for a "policy correction response" will be sent to the TAC stating: *With regard to the policy or procedural violation(s), you must acknowledge and respond within thirty (30) days indicating changes your agency will make to improve your procedures. Failure to respond within thirty days will result in your agency being reported to the Operations Sub-Committee of the ACIC Supervisory Board for recommendation of action to be taken.*
3. The response must be completed within the Audit Software documenting 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.
4. 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.

CJIS IT Audits (Criminal and Noncriminal Agencies)

The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information. The CJIS Security Policy is also used to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

The policy areas focus upon the data and services that the FBI CJIS Division exchanges and provides to the criminal justice community and its partners. Each policy area provides both strategic reasoning and tactical implementation requirements and standards. While the major theme of the policy areas is concerned with electronic exchange directly with the FBI, it is understood that further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges. Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life. Not every consumer of FBI CJIS services will encounter all of the policy areas therefore the circumstances of applicability are based on individual agency/entity configurations and usage. Use cases within each of the policy areas will help users relate the Policy to their own agency circumstances.

The policy areas are:

- Policy Area 1- Information Exchange Agreements
- Policy Area 2- Security Awareness Training
- Policy Area 3- Incident Response
- Policy Area 4- Auditing and Accountability
- Policy Area 5- Access Control
- Policy Area 6- Identification and Authentication
- Policy Area 7- Configuration Management
- Policy Area 8- Media Protection
- Policy Area 9- Physical Protection
- Policy Area 10- Systems and Communications Protection and Information Integrity
- Policy Area 11- Formal Audits
- Policy Area 12- Personnel Security
- Policy Area 13- Mobile Devices

I. PREPARATION

a. Your agency will be assigned the ACIC CJIS IT Audit Report and ACIC Systems PreAudit Questionnaire at the same time.

b. Once your agency has been assigned an audit, the TAC orNAC (Noncriminal Justice Agency Coordinator) will receive an email notification stating: *Your agency has been assigned an Audit. Please login to the CJIS Audit system to complete this audit.* Your User Name/Password for the ACIC CJIS IT Audit Report will be the same credentials as provided in the pre-audit letter.

c. The ACIC CJIS IT Audit Report will need to be completed within the audit software in less than 30 days.

II. SANCTIONS

Network Quality and Accountability/Policies and Procedures

As a result of the audit 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 the audit software in less than 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 may 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.

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

- ***a.*** Thirty days before an audit, the Noncriminal Justice Agency Auditor will send the agency a pre-audit letter to introduce the audit date, the ACIC auditor, and the User ID and Password that the NAC will need to log into the online auditing software. This letter will be sent to the. An additional letter introducing the audit date will be sent to the administrator.
- ***b.*** Once your agency has been assigned an audit, the NAC will receive an email notification stating: *Your agency has been assigned a Pre-Audit Questionnaire/Audit. Please login to the CJIS Audit system to complete this audit.* Your User Name/Password for the CJIS Audit System is provided in the pre-audit letter.
- ***c.*** 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 within the audit software. Once the report is finalized, an email will be sent to the chief official and/or NAC advising that "*An audit has been reviewed for your agency. Please login to the CJIS Audit system to view this audit. "* The acknowledgement of this audit report shall be submitted within 15 days of receiving the *review response notification*. In addition, copies will be maintained by ACIC. The 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 the audit software in less than 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 may 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.