Arkansas Community Correction

Two Union National Plaza Building
105 West Capitol, 3rd Floor
Little Rock, AR 72201-5731
501-682-9510 (office) 501-682-9513 (fax)

Administrative Directive: 16-04 ACIC/NCIC Criminal Information Systems

To: Arkansas Community Correction Employees

From: Sheila Sharp, Director

Supersedes: AD 05-07

Approved: Signature on File **Effective: June 1, 2016**

I. APPLICABILITY. This policy applies to Arkansas Community Correction (ACC) employees.

II. POLICY. It is ACC policy to comply with all applicable provisions of laws, rules, regulations and guidelines pertaining to access and use of ACIC/NCIC crime information systems and messages transmitted through the National Law Enforcement Telecommunications System (NLETS).

III. BACKGROUND INFORMATION.

A. Arkansas Crime Information Center (ACIC). ACIC is the central repository for Arkansas crime information. It administers the state's automated criminal justice information system and serves as the central access and control agency for Arkansas input, retrieval, and exchange of criminal justice information in the National Crime Information Center (NCIC) or its successor and National Law Enforcement Telecommunications System, Inc. (NLETS) or its successor.

B. Criminal History Information. Criminal history information maintained in the ACIC/NCIC database includes records compiled by ACIC on certain individuals consisting of names and identification data, notations of arrests, detentions, indictment information, or other formal criminal charges.

C. National Crime Information Center (NCIC). NCIC is the Federal Bureau of Investigation's (FBI) computerized information system that provides criminal justice information to local, state and federal criminal justice agencies.

D. National Law Enforcement Telecommunications System, Inc. (NLETS). NLETS is a National computer-controlled message switching service responsible for the routing and relaying of interstate messages.

E. Originating Agency Identifier (ORI). The ORI is a unique number assigned by the FBI to each law enforcement/criminal justice agency that identifies the agency accessing criminal history information systems.

F. Site Terminal Agency Coordinator (TAC). The Site TAC is appointed by the Director to interact with ACIC auditors and to ensure security of computers used to access the ACIC system and to perform other duties outlined in this policy.

G. Terminal Agency Coordinator (TAC). The TAC is appointed by the Director to serve as the agency liaison with ACIC and to perform duties outlined in this policy.

IV. GUIDANCE.

A. Access and Use of Information.

1. Purpose. Information obtained from ACIC, NCIC and NLETS must only be for the purpose of performing functions of investigation, apprehension, detention, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders; criminal identification activities; the collection, maintenance and dissemination of criminal justice information; ACC employment purposes; conducting background checks on applicants and as authorized.

2. Training. Users must be trained before accessing criminal justice information, refer to details in this policy.

3. Log. A criminal history secondary dissemination log provided by ACC or ACIC must be maintained for at least one year on all secondary disseminations of criminal history information. Secondary dissemination is distributing criminal history information outside ACC to other criminal justice or law enforcement agencies.

4. Disposal. Burning and shredding are the authorized methods for disposal of information printed from ACIC and NCIC files and NLETS messages.

5. Penalties. Release of information to an unauthorized person or obtaining information for an unauthorized purpose may result in fines and/or imprisonment as prescribed in Arkansas law section 12-12-212. Additionally, disciplinary action up to and including employment termination may be taken.

6. Right of Challenge. An offender has a right to challenge the contents of his or her criminal history record in ACIC. Requests should be addressed to the Administrator of the ACIC Criminal History Division.

B. Message Switching. Only official business messages that meet established guidelines in the ACIC Operator's Manual may be transmitted over ACIC or NLETS.

C. Security, Inspections and Audits.

1. Security. Prevent unauthorized access and protect computer equipment, documentation and records. Only authorized personnel may access the ACIC system.

2. Inspections and Audits. Offices where the ACIC system is accessed are subject to periodic ACIC/FBI security inspections and audits. The Site TAC must:

   a. assist ACIC personnel in audits, security checks, and related matters
   b. complete pre-audit questionnaires. Submit the completed pre-audit questionnaire to ACIC and send a copy to the Chief Deputy Director and agency TAC
   c. upon receipt of an audit report, send a copy to the Chief Deputy Director and agency TAC.

   d. prepare a response to the audit report and send it to the Chief Deputy Director for approval and to the agency TAC for his/her information.
   e. when directed by the Chief Deputy Director, send the audit response to ACIC; ensure the approved-final copy is provided to the Chief Deputy Director and agency TAC.
   f. act to resolve any discrepancies. Refer to the ACIC Audit Program/Audit Process document for details.
   g. Ensure corrective action is taken on deficiencies as stated in audit reports. Send appropriate responses to ACIC and provide a copy to the agency TAC and Chief Deputy Director.

D. Director's Responsibilities. The ACC Director must appoint appropriate staff for the positions of "Terminal Agency Coordinator" and "Local Agency Security Officer" and inform ACIC.

E. Chief Deputy Director. The Chief Deputy Director will process audit reports as described and will maintain a file of reports and submitted responses. He/she will review requests for ACIC direct-access users.

F. Terminal Agency Coordinator (TAC). The Terminal Agency Coordinator must perform the following duties:

1. Serve as liaison to ACIC
2. Serve as ACC representative for the ACIC user group
3. Perform duties described in the ACIC publication entitled "Duties and Responsibilities of the ACIC Terminal Agency Coordinator" with the exception of duties expressly listed for others in this policy
4. Maintain a list of all Site TACs.
5. identify and document how ACC information systems are connected to the state computer network.
6. obtain ACIC approval for any computer system
   a. before implementing new equipment that connects to the ACIC CJIS (Criminal Justice Information System)
   b. before making any changes or relocating equipment that connects to the ACIC CJIS.
   c. inform ACIC of location and ID of device.

G. Local Agency Security Officer (LASO). LASO duties are described in the ACIC publication entitled "Arkansas Crime Information Center System Regulations." However, for ACC many of the LASO duties are delegated to others in this policy. The ACC LASO will be a designated person in the IT section. He/she will ensure only employees who are approved by the Chief Deputy Director have a license key on their computer. He/she will be the only ACC employee authorized to contact ACIC to request user license keys. He/she will ensure network security to include coordinating system changes with ACIC in advance and obtain necessary ACIC approvals.

H. ACC-ACIC Control Center Coordinator. The ACC Control Center Coordinator is primarily responsible for the proper operation of the ACC-ACIC Control Center located at CACCC. He/she must ensure an adequate number of staff is trained as Advanced Operators and that an Advanced Operator is always available at the center.

I. ACC-ACIC Control Center Operations.

1. Location. ACC must maintain a 24-hour, 7 day-a-week ACC-ACIC control center operation at the Central Arkansas Community Correction Center (CACCC).

2. Processing Warrants. ACIC system operators at the Parole Board are responsible for entering ACC abscond warrants into the ACIC/NCIC system. CACCC enters escape warrants for escapes from ACC facilities and reentry programs. Entries in the ACIC and NCIC must be substantiated by official warrant documents and the documents must be retained on file until the entry is removed from the crime information system.

3. Monthly Validation of Warrants. CACCC must provide monthly validation of warrants they have entered into ACIC. The Parole Board will validate warrants they have entered. The Parole Board sends a copy of the warrants they check to CACCC so CACCC can purge obsolete paper copies of warrants.

4. Hit Confirmation Requests. A "Hit" is a positive response to an ACIC/NCIC inquiry that requires confirmation by ACC. ACIC operators at CACCC are responsible for responding to "Hit" confirmation requests. When the ACC-ACIC Control Center Operator receives a request for confirmation of a "Hit" from other law enforcement agencies, within 10 minutes the operator should respond to the hit or provide an approximate time a response can be expected. Providing a Hit confirmation may require an eOMIS (electronic Offender Management Information System) inquiry.

J. Area Managers, Center Supervisors and the Chief Deputy Director (for the Central Office). The Area Managers, Center Supervisors, and, for the Central Office, the Chief Deputy Director must:

1. serve as or designate another person as a "Site TAC" for his/her area(s) of responsibility; and notify the TAC of the appointed person.
2. bear overall responsibility for compliance with applicable aspects of this policy within his/her area of responsibility.
3. conduct pre-audits and process ACIC audits pursuant to this policy or ensure this work is done by a designee.
4. process requests as described in the paragraph entitled "ACIC Operators and ACIC Operator Authorizations."

K. Site TAC. Site TACs must:

1. ensure security of computers used to access the ACIC system.
2. distribute ACIC documents and materials to appropriate personnel.
3. process the "Request for ACIC Training" form to include completing the Security Clearance portion, sign the "Chief Official's Signature" block and as appropriate assist with scheduling the training.
4. ensure employees have current CJIS (Criminal Justice Information System) Security Training or Operator training before handling CJIS information.
5. conduct on-site compliance checks for his/her assigned Area/Center as necessary. and report any substantial discrepancies to the agency TAC and the Chief Deputy Director.
6. Perform duties described in the paragraph entitled "Security, Inspections and Audits."

L. ACIC Operators and ACIC Operator Authorizations. An ACIC Operator is an ACC employee who is trained and authorized for direct access to the ACIC system as either a "Basic Operator," who may only make inquiries, or an "Advanced Operator," who may make inquiries and enter information. ACIC operators must comply with all ACC, ACIC, NCIC and NLETS policies and procedures; inform the Site TAC of matters concerning ACIC training classes and changes in operator assignments, and assist with audits, security checks, and related matters. Area Managers must submit a request to the ACC Information Technology Section to add trained operators. Area Managers must also notify Information Technology when access is no longer needed. The Information Technology Section staff must keep track of the authorizations to ensure the log indicates which computers have security authentication codes that allow direct access.

M. eOMIS Access to ACIC Offender Information. It is possible to access ACIC information pertaining to offenders in eOMIS when granted permission. This access does NOT allow such things as searching for a license plate number. Area and Assistant Area Managers may submit a request to the ACC Research and Planning Section requesting employees have ACIC access through eOMIS. There is no limit on the number of employees granted this access. In the request the manager must attest that the employee is current in the required ACIC training as a "Basic Operator" or "Advanced Operator." Employees accessing ACIC information must comply with applicable ACC, ACIC, NCIC and NLETS policies and procedures; and inform the Site TAC of information security vulnerabilities and breaches.

N. CENSOR (Centralized Electronic Network of Sex Offender Registries). The ACC Sex Offender Services Area Manager must pre-approve of any ACC employee who needs access to CENSOR.

O. Training Requirements.

1. <u>ACIC Operator Training Requirements</u>. ACC staff designated as Basic or Advanced Operators must complete the required ACIC Basic/Advanced Operator training initially and again every two years.

2. eOMIS Access to ACIC Offender Information. ACC staff granted approval for access to ACIC offender information through eOMIS must complete the required ACIC Basic Operator (or Advanced Operator) training initially and again every two years.

3. CJIS Security Training Requirement. ACC employees who handle or view ACIC/NCIC criminal information must be current in ACIC/NCIC CJIS Security Training and must be retrained at a minimum of every two years. CJIS Security Training is incorporated in the Basic Operator and Advanced Operator training.

4. Conducting CJIS Training. Instructors must comply with requirements in the ACIC Training Policy.

5. CENSOR Training. ACC employees must have initial CENSOR (Centralized Electronic Network of Sex Offender Registries) training before being granted access to CENSOR and must be retrained a minimum of every two years.

P. Training Enrollment.

1. CJIS Security Training. Employees who need CJIS Security Training should send an ACC employee Training Request form to the Site TAC. The Site TAC will enroll employees in the on-line CJIS Security Training or will contact ACIC to obtain a password for use by the employee to access the training.

2. ACIC Operator, CENSOR (Centralized Electronic Network of Sex Offender Registries), TAC Training Requests. To request ACIC Operator, CENSOR, or TAC training, in addition to the ACC Training Request form, process the "Request for ACIC Training" form, available from the ACIC website, "Forms" tab. Send the ACIC form to the Site TAC who will coordinate scheduling of the training. Site TACs should forward the completed form to ACIC and may schedule people directly in an open class.

V. ATTACHMENT.

Criminal History Secondary Dissemination Log (ACIC Form 105)

Arkansas Crime Information Center
CRIMINAL HISTORY SECONDARY DISSEMINATION LOG

AGENCY: Arkansas Community Correction ORI:_____PAGE:____ of _____

Date	Time	Subject's Name, Race, Sex and DOB Or SID Number or FBI Number	Name, Rank/Title of person to Whom the Record Was Given	Reason for Request (Be Specific)	Person Making Dissemination

All criminal history obtained through ACIC, NCIC and III using this ORI must be entered in this log before being provided to another criminal justice agency. This log must be kept at least one (1) year from the earliest entry.

Revision date 5/2016 (Reference: ACIC/NCIC Criminal Information Systems Administrative Directive)