Division of Arkansas Crime Information
Arkansas Department of Public Safety

322 South Main Street, Suite 615
Little Rock, AR 72201
www.dps.arkansas.gov
501-682-2222

Mike Hagar
Secretary

Jeff Long
Director

Duties & Responsibilities

of the

Terminal Agency Coordinator

Arkansas Crime Information Center
322 South Main Street, Suite 615
Little Rock, AR 72201
(501) 682-2222

Revision
August 21, 2024

ACIC MISSION STATEMENT

The mission of the Arkansas Crime Information Center is to administer the state's automated criminal justice information system in an efficient and cost-effective manner so as to provide timely, accurate, and reliable data both to the public, as provided by law, and to local, state, and federal criminal justice agencies as an integral tool in the execution of their duties to protect the citizens.

DEFINITION

A Terminal Agency Coordinator (TAC) serves as a vital communication link between your terminal agency site and ACIC. This individual will act as the primary contact person for their agency. A TAC, among other duties, is responsible for ensuring quality record entries, assisting in agency audits, coordinating individuals for the appropriate level of training, and distributing all ACIC communications to agency personnel.

SECTION TITLES/TAC RESPONSIBILITIES

1. Definitions
2. TAC Training Requirements
3. Agency Contact Information
4. Audits
5. Employee Background Checks
6. Agency Employee Training Requirements
7. Validations
8. System Security
9. Person with Security Responsibilities (LASO) CJISSECPOL requirements

Definitions

CJISSECPOL (also known as ***CJIS Security Policy***) -The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of criminal justice services and information.

CJIS Security Addendum –An agreement between the Criminal Justice Agency (CJA) and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to systems that access or contain Criminal Justice Information (CJI). The Addendum limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require. Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function and shall be subject to the same extent of audit review as are local user agencies.

Direct Access user – a Criminal Justice Official that has successfully completed the ACIC/NCIC training requirements and has the authority to run queries, make entries or modify active entries in the NCIC system utilizing a direct access device.

Entering Terminal Agencies - Criminal Justice Agencies with direct access to the ACIC/NCIC system that makes entries into the various NCIC files (stolen guns, stolen vehicles, wanted persons, missing persons, violent persons, etc...)

Identity Proofing – the process used to verify a user's identity before they are configured for access to ACIC applications and criminal justice applications.

Indirect Access User - a Criminal Justice Official that has successfully completed the ACIC/NCIC training requirements and has the authority to receive information from the ACIC/NCIC system but does not have the authority to process their own transactions utilizing a direct access device.

Information Exchange Agreement – A formal agreement signed between Criminal Justice Agencies exchanging Criminal Justice Information (CJI). The agreement should outline the roles, responsibilities and data ownership between agencies and any external parties. It shall specify the security controls and conditions required to maintain system integrity.

Interstate Identification Index (III) - An automated listing of Criminal History Numbers from all 50 states. More specifically, Criminal History Record Information that is warehoused subsequent to the submission of fingerprint information.

Holder of Record Agreement – 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.

Management Control Agreement - an agreement that must been executed giving management control to a criminal justice agency in order for a non-criminal justice agency to have gain access to the ACIC/NCIC system. Management control is defined as the authority to set and enforce (1) priorities; (2) standards for selection, supervision, and termination of personnel access; and (3) policies governing operations, insofar as those policies apply to law enforcement communications and records.

Non-Entering Terminal Agencies - Criminal Justice Agencies that do not make entries into the various NCIC files. Primarily these agencies have direct access to the ACIC/NCIC files for queries only

Person with Security Responsibilities - Previously known as the Local Agency Security Officer(***LASO***)- responsibilities include (1) acting as the point of contact for information security matters; (2) responsible for agency adherence to the CJISSECPOL (3) responsible for reporting security incidents involving CJI or agency networks to the ACIC ISO (4) distribute security alerts to employees of the interface agency; (5) receive basic and on-going security training from ACIC; (6) assist the ACIC Information Security Officer (ISO) with security awareness training; and (7) assist state and federal auditors with technical audits in the interface agency

System Service Agreement – The chief official of each interface agency is required to sign a System Service Agreement, which outlines their duties and responsibilities concerning ACIC, NCIC, and NLETS policies and procedures.

Terminal Agency Coordinator (TAC) - serves as a vital communication link between your terminal agency site and ACIC. This individual will act as the primary contact person for their agency. A TAC, among other duties, is responsible for ensuring quality record entries, assisting in agency audits, coordinating individuals for the appropriate level of training, and distributing all ACIC communications to agency personnel.

User Authentication Method – the method used by an authorized user as they sign into a direct access device using either a Password or Token/PIN combination in order to identify themselves to the ACIC network.

Validations – The process that requires an examination of an agency's active NCIC records to confirm that records are complete, accurate, and still active. Proper validation is extremely important in limiting the potential for liability as a result of wrongful arrests and seizures.

SECTION 2

TAC Training Requirements

ACIC encourages all TACs to complete the specialized regional TAC training that is offered on an annual basis as well as recommends an advanced level of certification for TACs employed with agencies with NCIC record entries.

ACIC hosts a yearly User's Conference. 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 practices. It is expected that the TAC or an agency designee will attend the conference. Information and registration for the yearly conference can be found on the Department of Public Safety (DPS) website in the ACIC portion under ACIC Conference.

SECTION 3

Agency Contact Information

The agency TAC will use the appropriate forms and contact information to notify ACIC of changes within their agency. A new TAC should be designated immediately if the previous TAC is reassigned or is no longer employed with the agency. ACIC should be notified within 24 hours when an employee is terminated, resigns, or no longer needs access.

Changes in TAC	**TAC Designation Form**
Changes in Administration	ACIC.Operations@dps.arkansas.gov or notify assigned field agent
Address, Email, Phone Number Updates	**Agency Address Change/Update Form**
No Longer Employed (NLE) Personnel	**Request to Remove User** Form or Messenger **REMOVE** Form
Changes in "Person with Security Responsibilities"	Designate the individual in CJIS Online

All TAC forms can be obtained inside the Terminal Agency Coordinator (TAC) folder at: https://portal.acic.arkansas.gov/launchpad under the "CJIS Documents" tab

Audits

Every law enforcement agency with direct access to ACIC/NCIC is audited a minimum of once every three years. Additional audits may be conducted as needed if the 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 criticism or penalties.

Preparing for an ACIC Systems Audit – Entering Terminal Agencies

The ACIC Audit will consist of three parts:

• Pre-Audit Questionnaire

The audit coordinator will send the TAC a letter with the link to log into the audit software along with the username and password. The pre-audit questionnaire will cover the following areas: agency contact information, security, training, dissemination, quality control, validations, and hit confirmations.

Enclosed with this letter is also:

- ❖ A list of III transactions ran by your agency. An explanation of each III is required. Documentation of the CCH explanation(s) will need to be maintained onsite and provided to the auditor at the time of the audit.
- ❖ Instructions for accessing your agency's user authentication methods (UAM) will also be provided.
- ❖ A list of employees that have completed a fingerprint-based background check. Documentation and the ASP results letter on these individuals with unescorted access to areas containing criminal justice information should be provided to the auditor at the time of the audit.

• Verifying Documentation

The auditor will ensure that all training lists and documents are up to date. A System Service Agreement with current administrators' signatures is required. Other agreements may include Holder of the Record Agreements, Management Control Agreements, or Information Exchange Agreements. These agreements should also include current administrators' signatures.

Your agency will need a current policy and procedure for adding or removing personnel when there is any change in employment status. Other policies and procedures may include, if applicable, warrant entry policy, missing person entry policy, audit policy, dissemination policy, vehicle entry policy, training policy, and validation policy.

• NCIC Records Check

Your auditor will arrive at your agency with a random sampling of current NCIC vehicles, boats, parts, protection orders, violent persons, gang members, wanted persons, and missing persons. The auditor will review warrants, protection orders, case reports (with supplements), and any other supporting documentation. The ACIC auditors will check for validity, accuracy, completeness, and timeliness of each record, along with proof of second party checks.

Preparing for an ACIC Systems Audit – Non-Entering Terminal Agencies

The ACIC Audit will consist of two parts:

• Pre-Audit Questionnaire

The audit coordinator will send you a letter with the link to log into the audit software along with your username and password. The pre-audit questionnaire will cover the following areas: agency contact information, security, training, dissemination, quality control, validations, and hit confirmations.

Enclosed with this letter also:

- ❖ A list of III transactions ran by your agency. An explanation of each III is required. Documentation of the CCH explanation(s) will need to be maintained onsite and provided to the auditor at the time of the audit.
- ❖ Instructions for accessing your agency's user authentication methods (UAM) will also be provided.
- ❖ A list of employees that have completed a fingerprint-based background check. Documentation and the ASP results letter on these individuals with unescorted access to areas containing criminal justice information should be provided to the auditor at the time of the audit.

• Verifying Documentation

The auditor will ensure that all training lists and documents are up to date. A System Service Agreement with current administrators' signatures is required. Other agreements may include Holder of the Record Agreements, Management Control Agreements, or Information Exchange Agreements. These agreements should also include current administrators' signatures.

Your agency will need a current policy and procedure for adding or removing personnel when there is any change in employment status. Other policies and procedures may include, if applicable, warrant entry policy, missing person entry policy, audit policy, dissemination policy, vehicle entry policy, training policy, and validation policy.

All audit documents, including, *How to Successfully Complete an ACIC Audit*, can be obtained inside the Audit folder at:
https://portal.acic.arkansas.gov/launchpad under the "CJIS Documents" tab

Qualified Employee Background Checks

The minimum authorized age for an individual operating an ACIC access device is 18. Any person operating an ACIC access device also must be a U.S. citizen, or a legal alien specifically approved by ACIC. 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.

The agency TAC must ensure a criminal history background check has been completed on all agency personnel that will handle ACIC/NCIC/CJIS information by performing a QW transaction followed by a QH and QR using purpose code J. This is considered one of the first necessary steps in determining qualification of access to CJIS information or areas where CJI is stored or housed.

Conviction Type	Access	No Access
Felony		X
Felony (sealed)		X
Felony (pardoned)	X	
Misdemeanor (except for crimes of deception)	X	
Misdemeanor (conviction of a crime of deception)	X**	X*
Misuse of the ACIC system (conviction class D felony or class A misdemeanor)		X
Terminated due to misuse of ACIC system		X
Criminal history shows an arrest, but the charge severity cannot be determined		X***
Criminal history shows an arrest but there is no disposition		X***

*Deception is defined as the act of misleading another through intentionally false statements or fraudulent actions. Examples of deception are any type of fraud, criminal impersonation, and theft.

**Access will be granted if the subject does not have any charges on their record for the past 10 years.

***It is the hiring agency's responsibility to contact the appropriate law enforcement or court officials to determine if the disposition would disqualify the individual from gaining access.

This list is not all-inclusive.
Contact ACIC for situations that are outside the scope of this document.
ACIC.Operations@dps.arkansas.gov

All criminal justice agencies must verify a user's identity before they are authorized for configuration to access to any CJIS application, ACIC application or any electronic system containing criminal justice information. This may include agency domains, reporting systems, or record management systems. This process is known as Identity Proofing. The purpose of Identity Proofing and ID collection is to verify the applicant's identity by validating

the presented ID and binding the ID to the applicant's CJIS system credentials. Identity proofing is not used to determine eligibility for access. The Identity Proofing Procedure requirement can be found on the CJIS launchpad in CJIS documents tab under the "Security Documents" and "CJIS Example Policies" folder.

Eligibility for access to any CJIS application, ACIC application or any electronic system containing criminal justice information (*including agency domains, reporting systems, or record management systems*) cannot be determined until the results of a national fingerprint-based criminal history record check has been completed. The agency TAC must ensure a state and national fingerprint-based background check has been submitted prior to granting access to any personnel who may have unescorted access to criminal justice information. The blue applicant fingerprint card or an electronic fingerprint submission must be completed for agency personnel and forwarded to the Arkansas State Police AFIS Department.

Arkansas State Police AFIS Department
One State Police Plaza Drive
Little Rock, AR 72209
501-618-8500

Applicants that are subject to a national fingerprint-based criminal history record check for criminal justice employment must be provided the CJA Privacy Rights Consent and Challenge document. This document explains the applicant's Privacy Rights, as well as the process that must be followed in order to challenge the accuracy and completeness of the FBI criminal history record information used in determining employment qualification. This document can be found in the "TAC Section" of the "CJIS Documents" area of the CJIS Launchpad.

**The perspective employee may not be granted unescorted access until the results of the fingerprint-based background check have been received and verified that no disqualifying charges or dispositions are present.

It is recommended that the agency resubmits individual background checks and fingerprints every five (5) years.

SECTION 6

Agency Employee training requirements

All individuals directly operating an ACIC access device (*including mobile devices*) or have indirect access to criminal justice information (*ACIC printouts or electronically stored data*) must be trained. When a new employee is hired or assigned to an ACIC workstation, the appropriate level of training must be achieved.

- **CJIS Security Training Indirect Access:** The TAC is set up as the Local Agency Admin and will create a CJIS Online account with the proper role of training through cjisonline.com. The TAC should review the CJIS Online Certification Expiration Report monthly to ensure all agency accounts (*to include staff and contractors*) are trained and current. All users are required to be retrained annually.
  Examples of individuals with indirect access who may need the CJIS Online Certification: jailors, janitors, IT staff (agency or contractors), maintenance personnel, court clerks, judges, prosecutors, chief officials, or officers who do not operate an ACIC access device

- **CJIS Security Training Direct Access:** CJIS Security Training for direct access users is managed in nexTEST. These users will need to be deactivated in cjisonline.com once becoming a direct access user. Direct access users will be required to take the CJIS Security Training prior to any ACIC certification or recertification. To register a user for direct access, the TAC will complete the Training Request Form or TRAINREQ including the appropriate training needed for new user.
  The form must be completed in its entirety to prevent delaying the user from gaining access to the system. Once the Training Request Form has been received by the ACIC Training Division, a confirmation email will be sent to the TAC. The new user will be given a User ID, temporary password, and granted access for on-the-job training with a certified operator only. Once the user has obtained their User ID and password, they must log into nexTEST and complete the Security Training and Security Test prior to accessing any system containing CJI. (Users are required to be retrained annually.)

- **Basic Certification:** Users should complete all 4 of the ACIC Basic Modules (1-4) online via the NexTEST software within 6 months of assignment to a position that requires direct access. The CJIS Security Training/Test must be completed prior to accessing a system that houses, stores, or transmits CJI and before the user completes ACIC Basic Modules 1-4. The new user should also complete the Beginner's Guide to ACIC in conjunction with the online Basic certification course.
  Once the Security Training/Test is complete and the user has successfully passed each of the 4 Basic module certification tests with a score of 70% or higher, the user will be certified as a Basic user. The TAC will have access through the nexTEST Agency Login to monitor their users' certification scores. Once this process has been completed local agency personnel must entered the CLEST training hours into the acadis portal.

- **Advanced Certification:** A current certified basic user must be registered before attending the Advanced Certification Course. There is a mandatory waiting period of 30 days between completion of the Basic Certification Course and the Advanced Certification Course. To register a user for advanced access, the TAC will complete the Training Request Form or TRAINREQ using the ACIC Messenger software.
  Once the Training Request Form has been received by the ACIC Training Division, they will advance the user's privileges to an advanced status. This will depend upon whether or not the user has successfully completed their Security Training, Security Test, and their online Basic Certification course (modules 1-4). Once all training/testing requirements have been met, the user account will be set to begin the "ACIC Advanced Pre-Attendance Online Course". The user will sign into nexTEST and take the training and then click on the NCIC Certification tab and take the ACIC Advanced Pre-Attendance Test. The user should stop at that point. Once the Advanced Pre-Attendance Online Course training/testing requirements have been met, the user account will be set to begin the Day 1 Test for the in-person advanced class. After the user has successfully passed this course, the ACIC Training Division will enter the appropriate number of CLEST training hours into the acadis portal.

- **Basic & Advanced Recertification:** ACIC/NCIC requires that all users recertify annually. This can be accomplished by logging into nexTEST and taking the CJIS Security Training then completing either the Basic Recertification Test or the Advanced Recertification Test. Once a user has been expired for a period of 1 year, they will not be able to recertify and must complete the online ACIC Basic Course (modules 1-4) to begin the certification process again.

- **CJIS Security Recertification (Indirect Access):** ACIC/NCIC requires that all users recertify annually. This can be accomplished by logging into CJIS Online and completing the CJIS Security Training and Test.

Notify the ACIC Training Division as soon as possible if a student is unable to attend a scheduled training class.

Training:	Class Type:	CLEST Credit:
CJIS	Online	N/A
Basic	Online	4 Hours
Advanced	In Person	24 Hours
Recertification	Online	N/A

All training information, dates, and training guides can be obtained at: https://portal.acic.arkansas.gov/launchpad under the "CJIS Training" tab.

SECTION 7

Validations

Validation requires an examination of your active NCIC records to confirm that records are complete, accurate, and still active. Proper validation is extremely important in limiting the potential for liability as a result of wrongful arrests and seizures. All agencies with entries in NCIC are required to participate in the validation process. Failure to follow the process could result in your agency's records being purged from the system or other sanctions imposed by the ACIC Supervisory Board.

The validation process is as follows:

1. ACIC will post a file in the messenger software containing records scheduled for validation for each originating agency (ORI). A message will be distributed via the CJIS Launchpad in the News & Information section with the records that are available and when they are due. Your agency will receive 1/12 of all active records to validate on a monthly basis.
2. Use the **QVAL** to query your monthly validation list as well as the monthly validation list of any other agencies you are responsible for preforming validations for.
3. A **QVAD** will provide the NIC numbers of records needing validation. Compare each record with the supporting documentation and ensure that all records are accurate and contain all available information. Review fresh transaction returns on all entries such as QW, QH, QWI, QSOF, etc.

4. Follow up on all records by contacting the victim, complainant, prosecutor, court, and/or nonterminal agency to confirm the record's status. In the event the ORI is unable to make contact with a victim or complainant, a determination must be made, based on the best information available, whether or not to keep the entry in NCIC according to your agency's policy.
5. Your agency should use the **VAL** to manually validate each individual record or the **BVAL** to batch validate all records within each file.
6. In instances where a record has been cleared after the validation list was posted in the messenger software, a DVAL should be used to delete the record from the validation software list. This transaction will not delete the record from NCIC, only from the validation list.
7. Remove records that are no longer valid.
8. Once the validation process is complete, the agency should perform a second **QVAL** to ensure all records have been validated.
9. If the QVAL return indicates there are records remaining that were not validated, a **QVAD** should be ran again in order to find the NIC#s of the unvalidated records. A query should be ran on each of the remaining NIC#s to determine if the record(s) are still active in the NCIC system.
    - *If the record is still active in NCIC, the record must be validated individually using the **VAL** transaction*
    - *If the NIC# produces a return that indicates "No Record on File", the DVAL transaction can be ran, which will remove the record from the validation list.*
10. Once this process has been completed another **QVAL** should be ran to ensure all records have been validated.

File Type:	Contact:	Process:
Warrants	District or Circuit Court Prosecuting Attorney	verify that arrest warrants are still active and have not been recalled or served
Protection Orders	District or Circuit Court	verify that orders are still active and have not been dismissed
Stolen Property	Reporting Party	verify that property is still missing, and recovery has not been made
Missing Persons	Reporting Party	verify that the person is still missing and has not returned
Article (Public Safety Items)	Reporting Law Enforcement Agency	verify that property is still missing, and recovery has not been made
Violent Person	Reporting Law Enforcement	Review and update the person information that is on file and in ACIC, verify status with the entering agency

All validation documents can be obtained inside the Validations folder at: https://portal.acic.arkansas.gov/launchpad under the "CJIS Documents" tab

SECTION 8

System Security

On-site security inspections will be conducted on all interface agencies to ensure compliance with the ACIC System Service Agreement, as well as ACIC, NCIC, and NLETS security policies. The TAC should work in conjunction with the **Person with Security Responsibilities** [Local Agency Security Officer (***LASO***)] to ensure security of ACIC equipment and the information obtained from the ACIC System.

Security includes but is not limited to the following:

1. Ensure your agency has a designated Person with Security Responsibilities (LASO)
2. Read and be familiar with the CJIS Security Policy and the ACIC System Regulations
3. Ensure that unauthorized persons are not allowed in the area of your ACIC workstation or other ACIC equipment unless escorted by authorized personnel
4. Ensure files containing ACIC information are protected from unauthorized persons
5. Ensure monitors displaying ACIC information are positioned in a manner protecting information displayed
6. Ensure that departmental personnel do not attempt to make changes to the ACIC equipment (software)
7. Ensure disposal of all ACIC documentation is done by burning or shredding using a crosscut shredder
8. Instruct all personnel on the proper dissemination of ACIC information
9. Contact ACIC personnel if there is a request for information (FOIA) and the validity or authority of that individual is in question
10. Educate users in memorized secrets (password/pin) security
11. Ensure the Person with Security Responsibilities (LASO) notifies your agency administrator and your local ACIC Field Agent of any suspected security incident
12. Submit a network diagram with any changes, additions, or removals to the agency's network (this includes relocation of access devices)
13. Ensure that all agreements are up-to-date with current administrators' signatures (*examples: System Service Agreement, Holder of the Record Agreements, Management Control Agreements, Information Exchange Agreements, etc.)*
14. Review all the department's internal policies related to ACIC (examples*: entry policies, security policies, validation policies, etc*.)

All security manuals and regulations can be obtained at: https://portal.acic.arkansas.gov/launchpad under the "CJIS Manuals" tab or at https://www.dps.arkansas.gov under Crime Information Center; Resources; Workstation & Terminal Information

Agreements and sample policies can be obtained at: https://portal.acic.arkansas.gov/launchpad under the "CJIS Documents" tab

Specific documents related to TAC Duties & Responsibilities can be found at: https://portal.acic.arkansas.gov/launchpad under the "CJIS Documents" tab listed in the "TAC" folder

To report a security incident within your agency: https://www.dps.arkansas.gov under Crime Information Center; Forms; Workstation & Terminal; Information Security Incident Report

Designation of Terminal Agency Coordinator

_____
Agency Name & Agency ORI

I hereby designate _____ to serve as Terminal Agency Coordinator (TAC) for this department.

I understand that a TAC is expected to be the primary liaison between my department and ACIC. The TAC will actively represent my department on matters relating to ACIC and be familiar with the records system and communication needs of my department. They will be responsible for receiving information from ACIC and appropriately handling or disseminating that information. The TAC will also keep ACIC informed on our training needs and other matters relating to the use of ACIC/NCIC/NLETS.

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

_____	_____	_____
Chief Official Signature	Title	Date

Acknowledgement of Duties by the Terminal Agency Coordinator

I, _____, have read and understood the TAC Duties and Responsibilities document. I am willing to serve as Terminal Agency Coordinator (TAC) for my agency.

_____	_____	_____
TAC Signature	Title	Date

Contact information for designated TAC:

Username for ACIC:	
TAC's Phone Number:	
TAC's Email:	

Contact information for designated assistant TAC (if applicable):

Username for ACIC:	
Assistant TAC's Phone Number:	
Assistant TAC's Email:	

Email the completed form to: ACIC.Training@dps.arkansas.gov