

 <p>ARIZONA DEPARTMENT OF CORRECTIONS</p> <p>DEPARTMENT ORDER MANUAL</p>	<p>CHAPTER: 100</p> <p>AGENCY ADMINISTRATION/MANAGEMENT</p>	<p>OPR:</p> <p>OPS SS PS</p>
	<p>DEPARTMENT ORDER: 121</p> <p><i>ARIZONA CRIMINAL JUSTICE INFORMATION AND IDENTIFICATION SYSTEM</i></p>	<p>SUPERSEDES:</p> <p>DO 121 (10/19/06)</p> <p>EFFECTIVE DATE:</p> <p>AUGUST 21, 2008</p> <p>REPLACEMENT PAGE REVISION DATE:</p> <p>MAY 24, 2011</p>

## TABLE OF CONTENTS

PURPOSE	
RESPONSIBILITY	
PROCEDURES	
121.01	SYSTEM SECURITY OFFICER ..... 1
121.02	ACJIS LIAISONS ..... 2
121.03	ACJIS OPERATOR CERTIFICATION ..... 3
121.04	CRIMINAL JUSTICE PRACTITIONER ..... 5
121.05	DOCUMENTATION ..... 6
121.06	DISSEMINATION ..... 7
121.07	APPLICATION OF INFORMATION..... 8
121.08	USE AND RESTRICTIONS ..... 8
121.09	VIOLATIONS ..... 9
121.10	ARIZONA AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM (AZAFIS) ..... 9
121.11	AUDITS OF AZAFIS IDENTIFICATION SYSTEMS ..... 11
121.12	AZAFIS IDENTIFICATION SYSTEM USE, RESTRICTIONS AND VIOLATIONS ..... 11
121.13	OPTICAL PRINT AND PHOTO IMAGE SUBSYSTEM (OPPIS) ..... 12
	DEFINITIONS ..... 12
	AUTHORITY..... 14

## PURPOSE

This Department Order establishes the use of the Arizona Criminal Justice Information System (ACJIS), Mug Photo Interface Software (MPI), Electronic Fingerprint Equipment (Live Scan), Instant Identification (Fast ID), and Optical Print and Photo Image Subsystem (OPPIS). These systems are used for the positive identification, collection, storage, retrieval and dissemination of documented criminal justice information. This information shall be protected to ensure legal and efficient use. Employees operating any of the equipment and/or software shall be trained, tested and certified. Employees reviewing any material displayed on these systems shall be trained in the legal aspects of information.

## RESPONSIBILITY

**Arizona Criminal Justice Information System (ACJIS)** - The Deputy Director, Division Directors, Wardens, Deputy Wardens, Bureau Administrators and the Contract Beds Operations Director shall appoint a staff member as the ACJIS Liaison for each ACJIS site.

The Chief Information Officer shall appoint a System Security Officer.

ACJIS Operators, Criminal Justice Practitioners and the System Security Officer are certified and approved by the Control Terminal Agency (CTA) which is the Arizona Department of Public Safety (DPS).

The Deputy Director, Division Directors, Wardens, Bureau Administrators and the Contract Beds Operations Director shall ensure that:

- All ACJIS computers and printers are located in such a manner that only authorized personnel are able to read the monitor display and/or printed material. The Central Office Contract Beds office shall be the only Contract Beds site to have an ACJIS computer.
- Computers, printers and manuals are located/secured in areas in which only authorized personnel have access. Manuals shall be located near computers and printers for operator use.
- All changes regarding the equipment connected to the ACJIS network are coordinated with the Control Terminal Agency, through the System Security Officer.
- Protection against unauthorized access is provided by appointing an ACJIS Liaison and ensuring that employees with access to the ACJIS network information, whether directly or indirectly, are identified on an authorization list submitted to and maintained by the System Security Officer.

**Arizona Automated Fingerprint Identification System (AZAFIS)** - The AZAFIS Site Administrator, under the direction of the Division Director for Program Services, is responsible for the oversight of all Department AZAFIS Identification Systems, to include the Mug Photo Interface subsystem (MPI), Live Scan, Fast ID and Optical Print and Photo Image Subsystem (OPPIS) and shall coordinate the use of these systems with outside agencies and vendors. All changes regarding equipment connected to any of the identification systems shall be coordinated with the Control Terminal Agency through the AZAFIS Site Administrator.

## PROCEDURES

**121.01 SYSTEM SECURITY OFFICER** - A staff member who ensures that the Department's staff accessing the ACJIS network is in compliance with all applicable laws, rules and regulations governing use of that information. The System Security Officer (SSO) shall act as the liaison between the user agency and the Control Terminal Agency (CTA). All requests regarding the use of the ACJIS/NCIC system shall be coordinated through the SSO. The SSO shall:

- 1.1 Monitor system usage.
- 1.2 Enforce system discipline.
- 1.3 Ensure that operating procedures are followed.
- 1.4 Serve as a central point within the Arizona Department of Corrections for all ACJIS issues to include:
  - 1.4.1 Record validations.
  - 1.4.2 Quality control matters.
  - 1.4.3 Disseminating ACJIS manuals and other ACJIS publications.
  - 1.4.4 Security matters.
  - 1.4.5 Agency personnel authorization/training/certification.
  - 1.4.6 Maintaining a record of ACJIS Operators and Criminal Justice Practitioners.
  - 1.4.7 Providing the CTA with updated lists of ACJIS Operators and Criminal Justice Practitioners as changes occur.
  - 1.4.8 Ensuring that ACJIS liaisons are requiring that ACJIS Operators and Criminal Justice Practitioners view the "ACJIS Overview" video, review this Department Order, and sign and date the Video and Department Order Viewing Log, Form 121-7. The log shall be included in the semi-annual report to the CTA.
  - 1.4.9 Processing requests for information/problems identified regarding ACJIS use.
  - 1.4.10 Coordinating with the CTA all requests for information, training and updates.
  - 1.4.11 Receiving Monthly Statistical Reports from the CTA, and routing them to the appropriate ACJIS Liaison for review.

**121.02 ACJIS LIAISONS - Shall:**

- 1.1 Prepare and forward a record of authorized Criminal Justice Practitioners and ACJIS Operators to the SSO.
- 1.2 Notify the SSO of changes in personnel as they occur.
- 1.3 Coordinate the training of prospective Criminal Justice Practitioners and ACJIS Operators.
- 1.4 Ensure that staff requesting authorization as a Criminal Justice Practitioner or ACJIS Operator completes a Request for Access to ACJIS, Form 121-5, and submit the form to the SSO. The liaison shall keep a copy of all requests.
- 1.5 Ensure that staff requesting authorization as a Criminal Justice Practitioner or ACJIS Operator views the "ACJIS Overview" video and this Department Order, and signs and dates the Video and Department Order Viewing Log. The logs shall be kept on file for six-month periods coinciding with the required semi-annual report. Report periods are set by the CTA and are May 1 to October 31 and November 1 to April 30. The logs shall be forwarded to the SSO with the semi-annual report.

- 1.6 Coordinate and schedule the ACJIS training with the CTA through the SSO.
- 1.7 Coordinate and administer the ACJIS Operator certification test to personnel training for operator status within six months from the date of the applicant's assignment to ACJIS-related duties.
- 1.8 Recertify ACJIS Operators within 30 days prior to their certification expiration date.
- 1.9 Maintain copies of ACJIS Operator certificates for audit purposes.
- 1.10 Ensure that ACJIS manuals and/or publications are updated.
- 1.11 Share new/updated information with all ACJIS Operators as it is received from the SSO.
- 1.12 Monitor ACJIS usage by reviewing the Monthly Statistical Reports.
- 1.13 Enforce system discipline.

### **121.03 ACJIS OPERATOR CERTIFICATION**

- 1.1 An employee requesting ACJIS Operator Certification shall:
  - 1.1.1 Have a bona fide job-related need for certification.
  - 1.1.2 Submit a "Request for Access to ACJIS" through their chain of command to the appropriate ACJIS Liaison.
  - 1.1.3 View the "ACJIS Overview" video and read this Department Order.
  - 1.1.4 Sign and date the "Video and Department Order Viewing Log."
- 1.2 ACJIS Operator certifications are divided into the following four levels:
  - 1.2.1 Level A - The certification test consists of 50 questions. Maximum testing time is two hours. This level is for Operators that enter records into ACJIS, as well as modify, clear, cancel and/or locate records. These Operators also interpret responses. Level A certification is limited to the SSO, personnel assigned to the Central Office Communications Center and staff in the Warrants Unit and the Sex Offender Coordination Unit.
  - 1.2.2 Level B - The certification test consists of 25 questions. Maximum testing time is one hour. This level is for Operators who inquire into the ACJIS network and interpret responses. These individuals do not enter or update records.
  - 1.2.3 Level C - Not applicable for the Department. This level is for Operators who use Mobile Digital Computers (MDC) only.
  - 1.2.4 Level D - This certification test consists of ten questions. Maximum testing time is one hour. This level is for agency Information Technology personnel who work with the ACJIS interface system.
- 1.3 The SSO shall, before approving the request, conduct a current ACIC/NCIC criminal history check and send a request to the Background Investigations Unit to ensure that a fingerprint card has been submitted to the DPS. The SSO shall notify the CTA, in writing, of any record located.

- 1.3.1 If a record of any kind is found, deny access pending review of the record in coordination with the CTA.
- 1.3.2 If the SSO and/or the CTA determine that access is not in the public interest, such access shall be denied and the requesting authority shall be notified, in writing, of the denial.
- 1.4 If approved, the ACJIS Operator shall be assigned a certification number by the CTA, through the SSO. The SSO shall add the operator to the Department's ACJIS Interface system and notify the operator of the information necessary to access the system. ACJIS Operators shall:
  - 1.4.1 Train at least one month, and no more than six months, during which time they routinely perform ACJIS operations with supervisory monitoring.
  - 1.4.2 Complete certification within six months from the date of assignment to ACJIS-related duties.
- 1.5 ACJIS Operator tests shall be administered in an "open book" manner allowing Operators to refer to the ACJIS Operating Manual during the test. Tests shall be administered on an individual basis only. Group testing or polling of answers is prohibited.
- 1.6 A certification number is the property of the ACJIS Operator. Operators are expected to know their number. Certification numbers remain on file with the CTA, and are not reassigned.
- 1.7 Certifications are valid for two years from the date of issue. Re-certification is required within 30 days prior to the date an Operator's certification expires.
  - 1.7.1 Operators who fail the re-certification test shall receive additional training by the ACJIS Liaison and/or the SSO and shall retest within 30 days.
  - 1.7.2 Operators whose certification has expired are not authorized to operate ACJIS computers.
  - 1.7.3 Operators who do not wish to recertify shall notify the SSO, through their ACJIS Liaison, prior to their certification expiration date. The assigned certification number shall be placed into inactive status by the CTA and shall be deleted from the Department's ACJIS interface system by the SSO.
- 1.8 If a certification or re-certification date is not met and an extension of the date is needed, the SSO shall submit a written request, to include a reason that the extension is needed, to the CTA.
- 1.9 Operators transferring to a different position in the Department and who wish to retain their certification shall contact the gaining ACJIS Liaison.
  - 1.9.1 Only when the transfer is into a position requiring ACJIS access shall the Operator be allowed to maintain certification.
  - 1.9.2 The gaining ACJIS Liaison shall forward a new Request for Access to ACJIS to the SSO.

- 1.10 An Operator, who has transferred into a position that requires that they view ACJIS information without having to have access to an ACJIS computer, shall become a Criminal Justice Practitioner rather than an operator. The employee shall contact the gaining ACJIS Liaison, who shall notify the SSO.
  - 1.10.1 The gaining ACJIS Liaison shall forward a new Request for Access to ACJIS to the SSO indicating a change of status.
  - 1.10.2 The Operator certification number shall be placed in inactive status by the CTA and the Operator deleted from the Department's ACJIS interface system by the SSO.
- 1.11 ACJIS Operators who have been placed on inactive status shall contact the ACJIS Liaison to request authorization to return to active status.
  - 1.11.1 Operators who request to be placed on active status are not required to retest or recertify unless the certification has expired or the level of certification is higher than the previous level held.
  - 1.11.2 The ACJIS Liaison shall notify the SSO when an Operator is returned to active status.
- 1.12 Operators who:
  - 1.12.1 Request to upgrade the certification level shall take the written exam for the desired level.
  - 1.12.2 Request to downgrade the certification level do not need to take an additional exam, but shall notify the SSO, through their ACJIS Liaison, of their intention.
- 1.13 Operators who change their name shall submit an updated Request for Access to ACJIS to the SSO, through their ACJIS Liaison.

#### **121.04 CRIMINAL JUSTICE PRACTITIONER**

- 1.1 An employee may be authorized to view and use information received from the ACJIS network, as a Criminal Justice Practitioner without having direct access to an ACJIS computer. The employee requesting authorization shall have a bona fide job-related need for viewing ACJIS information.
- 1.2 The employee shall complete and submit a Request for Access to ACJIS, through the chain of command, to the appropriate ACJIS Liaison. The ACJIS Liaison shall ensure that the employee views the "ACJIS Overview" video and this Department Order and forward the request to the SSO who shall approve or deny it.
- 1.3 Criminal Justice Practitioners transferring within the Department who wish to retain their status shall notify the gaining ACJIS Liaison, who shall notify the SSO of the transfer.
  - 1.3.1 The position shall require ACJIS access in order for the Criminal Justice Practitioner to retain the status.
  - 1.3.2 Criminal Justice Practitioners transferring to a position not requiring ACJIS access shall be placed on inactive status, and their name shall be removed from the list of authorized personnel. Personnel who have been placed on inactive status and who become eligible for reinstatement shall reapply.

- 1.3.3 The ACJIS Liaison at the new location shall forward a new Request for Access to ACJIS to the SSO.
  - 1.4 Criminal Justice Practitioners who change their name shall submit an updated Request for Access to ACJIS to the SSO, through their ACJIS Liaison.
- 121.05 DOCUMENTATION** - ACJIS sites are audited every three years by the CTA. Audit procedures are designed to assist in maintaining complete and accurate records and ensure that dissemination of information is made only to authorized individuals.
- 1.1 The ACJIS Operator shall document all ACJIS transactions.
    - 1.1.1 ACJIS activity shall be documented on the ACJIS Activity Log, Form 121-3.
    - 1.1.2 Transmission of Teletype messages using the Arizona/National Law Enforcement Telecommunications Systems (ALETs/NLETs) shall be documented on the ACJIS Teletype Message Log, Form 121-4.
    - 1.1.3 Secondary dissemination of ACJIS information shall be documented on the ACJIS Secondary Dissemination Log, Form 121-2.
  - 1.2 Requests for ACJIS information shall be submitted on a Criminal History Information Request, Form 121-1, completed by the Criminal Justice Practitioner making the request, or other approved written source such as a gate pass, visitation form, or the ACJIS Information Request list, Form 121-6.
    - 1.2.1 The purpose of a request shall be obtained from the requestor prior to accessing the ACJIS network.
    - 1.2.2 Telephone requests for information are not authorized. A Criminal History Information Request may be transmitted by facsimile (FAX) to the ACJIS Operator when it cannot be hand delivered.
  - 1.3 The ACJIS Operator's response to a request for information shall be documented on the Criminal History Information Request, or other approved documents as stated above.
  - 1.4 If an ACJIS report is released to an authorized requestor, the Operator shall initial and date the report, and note on it precisely how, when and to whom the information was released prior to providing the report to the requestor.
  - 1.5 ACJIS Operators shall maintain copies of information requests, ACJIS Activity Log Forms and Criminal History Information Requests outlined in this section for a three year period (coinciding with the audit time period).
    - 1.5.1 Reports shall not be filed or maintained inside the secure perimeter of a unit.
    - 1.5.2 Reports may be taken to a secured/restricted office that is located inside a unit, provided they are kept secured and out of sight of unauthorized persons, to include inmates and unauthorized staff.
    - 1.5.3 Reports of criminal history record information shall be maintained only for as long as there remains any possibility that action may be taken as a result of the information contained in the report. Then shall be destroyed as outlined in 1.6 of this section.

- 1.5.4 Reports of criminal history record information obtained from the ACJIS network shall never be maintained in any inmate record/file. (Printouts of warrant queries are not considered criminal history information and may be maintained in an inmate record/file.)
- 1.5.5 Printouts of identifying information shall be attached to outstanding warrants for audit purposes.
- 1.6 Approved methods for the destruction of printed documents obtained from the ACJIS network are:
  - 1.6.1 Shredding - The preferred method of destruction. The shredded material shall be properly disposed of.
  - 1.6.2 Burning - Shall only be used where it is legal and when it can be safely monitored and contained.
  - 1.6.3 Redacting - Is the process of eliminating identifying information contained within the data.

## **121.06 DISSEMINATION**

- 1.1 The existence or absence of criminal history information shall not be confirmed to any individual or agency not authorized to receive the actual information.
- 1.2 Any employee who is not authorized or approved shall not have access, whether directly or indirectly, to information obtained from the ACJIS network.
- 1.3 It is incumbent upon the Department to ensure that dissemination of information, directly or indirectly, is made only to authorized personnel. Any departure from this requirement warrants the removal of the ACJIS Operator from further access to the ACJIS network or information.
- 1.4 Any person, who knowingly releases or procures the release of information, other than as provided by applicable rules and regulations, is guilty of a Class 6 Felony and may be subject to disciplinary action as outlined in Department Order #601, Administrative Investigations and Employee Discipline.
- 1.5 Secondary Dissemination of information to another agency or department shall be documented in accordance with section 121.05, 1.2. The Originating Agency Identifier (ORI) of the requesting agency/department shall be used when accessing the ACJIS network for secondary dissemination.
- 1.6 Each employee who has access to ACJIS information shall be identified on an authorization list.
  - 1.6.1 This list is maintained by the SSO and the CTA and shall contain the individual's name, date of birth, date of hire and, if applicable, operator certification number. Additional information may include the individual's work location and the date the video was viewed.
  - 1.6.2 Each ACJIS Liaison shall maintain the authorization list for their area and submit revisions to the SSO as changes occur. Only those personnel authorized as Criminal Justice Practitioners or Certified ACJIS Operators shall receive information obtained from the ACJIS network.

- 1.7 Radio transmissions of criminal history record information shall be restricted to information necessary to effect immediate identification or to ensure the safety of the general public, staff and inmates. Such transmissions shall be avoided except in extreme emergency situations, such as riot, hostage, and escape.

## **121.07 APPLICATION OF INFORMATION**

- 1.1 ACJIS information shall be reviewed to determine a positive or negative response to the inquiry.
  - 1.1.1 A negative response shall not be relied upon as an indication that the person or property inquired upon is not wanted, missing or stolen, or that no criminal history record information exists.
  - 1.1.2 The receiving party shall use neither a positive or negative response as the sole basis for decision-making.
- 1.2 Name-only searches not supported by positive identification (fingerprints) may fail to result in the discovery of relevant records about the subject. When reasonable doubt exists as to whether information obtained from the ACJIS network is the correct subject, a fingerprint card shall be submitted to Background Investigations, or the SSO, with a Criminal History Information Request for technical comparison.
- 1.3 An individual shall be presumed not guilty of any charge/arrest for which there is no final disposition stated on the record or otherwise determined.

## **121.08 USE AND RESTRICTIONS**

- 1.1 The Department shall use the ACJIS network only for the following:
  - 1.1.1 The administration of criminal justice, i.e., the collection, storage and dissemination of criminal history record information.
  - 1.1.2 Entering/clearing/canceling warrants regarding inmates on parole absconder or home arrest curfew violator status.
  - 1.1.3 Conducting background investigations on prospective employees.
- 1.2 Any criminal justice agency that obtains criminal history information from the CTA, or through ACJIS, assumes responsibility for the security of the information and shall not secondarily disseminate this information to any individual or agency not authorized to receive this information directly from the CTA or originating agency.
- 1.3 Background Investigations shall process all background investigations of prospective employees, volunteers and contractors of the Department as outlined in Department Orders #204, Volunteer Services, #205, Contractor Security, and #602, Background Investigations.
- 1.4 Department of Transportation, Motor Vehicle Division files are accessible from the ACJIS network. Use of vehicle registration or drivers license information obtained from the ACJIS network is limited to law enforcement, criminal justice, or Motor Vehicle Division purposes only. Curiosity inquiries are forbidden.

## **121.09 VIOLATIONS**

- 1.1 Computer misuse or fraudulent use may subject a violator to the penalties outlined in Title 18, U.S. Code, Crimes and Criminal Procedure, and A.R.S. 13-2316.
- 1.2 The data stored in the ACJIS/NCIC computer system is documented criminal justice information and shall be protected to ensure correct, legal and efficient dissemination and use. The data stored is confidential and shall be treated accordingly. Any unauthorized request and/or receipt of ACJIS/NCIC material may result in criminal proceedings.
  - 1.2.1 Staff shall report suspected violations of this Department Order, ACJIS rules or regulations, or misuse of the ACJIS network to the SSO, who shall attempt to determine whether a violation or misuse has occurred.
  - 1.2.2 An employee who is not authorized/approved shall not have direct or indirect access, to information obtained from the ACJIS network.
- 1.3 The SSO shall provide assistance to any Warden or Bureau Administrator in any follow-up investigation into allegations of misuse and receive a copy of final reports on any such follow-up or investigation for the purpose of follow-up with the CTA and/or the Federal Bureau of Investigations NCIC audit team.

## **121.10 ARIZONA AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM (AZAFIS)**

- 1.1 All AZAFIS Identification System computers, printers and operating manuals shall be located in a secure area and positioned in such manner that only the authorized personnel have access to read the monitor, operating manual and printed material. The only Central Office sites authorized to have MPI systems are the Communication Center, Recruitment Unit for Selection and Hiring and Community Corrections.
- 1.2 Each Warden shall identify AZAFIS Identification System Operators for their complex. Unit Administrators shall ensure that only employees on the Authorization List have access to any of the identification system's equipment, computers, software and manuals. The AZAFIS Site Administrator maintains this list.
- 1.3 The AZAFIS Site Administrator shall:
  - 1.3.1 Ensure that only authorized staff have access to any of the AZAFIS Identification Systems and that all applicable laws, rules and regulations governing the use of the equipment and information received from the systems are in compliance.
  - 1.3.2 Be the Department's point of contact for all AZAFIS Identification Systems, to include MPI, Live Scan, Fast ID and OPPIS.
  - 1.3.3 Maintain a record of all AZAFIS Identification System Operators and advise DPS of all user changes.
  - 1.3.4 Update the AZAFIS Identification System User List quarterly and provide a copy to DPS.
  - 1.3.5 Maintain quality control use of the systems by auditing monthly reports provided by the vendors, disseminate all notices and information regarding the systems, and provide authorization and training for systems Operators.

- 1.3.6 Process requests for information and problems with the systems in a timely manner.
  - 1.3.7 Coordinate with DPS and appropriate vendors all requests for information, training and updates.
  - 1.3.8 Ensure vendors supply Monthly Statistical Reports and notify any routine problems.
- 1.4 Unit Administrators shall:
- 1.4.1 Notify the AZAFIS Site Administrator of any changes in personnel as they occur.
  - 1.4.2 Through the AZAFIS Site Administrator, coordinate the scheduling of Identification System Operators.
  - 1.4.3 Coordinate the training of the AZAFIS Identification System Operators at annual conferences and seminars.
  - 1.4.4 Ensure staff requesting authorization to use any AZAFIS Identification System complete and submit the AZAFIS Access Request, Form 121-8 to the AZAFIS Site Administrator.
  - 1.4.5 Within 8 hours of a user being removed as an AZAFIS Identification System user, notify the AZAFIS Site Administrator who will notify DPS.
- 1.5 Identification System User Training
- 1.5.1 Employees requesting to be a AZAFIS Identification operator shall:
    - 1.5.1.1 Have a bona fide job-related assignment.
    - 1.5.1.2 Complete and submit the AZAFIS Access Request form through their chain of command to the AZAFIS Site Administrator.
    - 1.5.1.3 If approved by the AZAFIS Site Administrator and the Unit Administrator, complete three weeks of on the job training from an AZAFIS Identification System user who has a minimum of one-year experience or has been approved by the AZAFIS Site Administrator.
  - 1.5.2 The AZAFIS Site Administrator shall complete the DPS form and enter the new user data into the AZAFIS web site and fax a copy of the form to DPS on the day of receipt.
  - 1.5.3 Operators who have forgotten their sign-on or password shall contact the AZAFIS Site Administrator for assistance. At no time shall a AZAFIS Identification System user directly contact DPS, unless they have prior authorization from the AZAFIS Site Administrator.
  - 1.5.4 Operators who transfer to a different position within the Department and wish to retain their AZAFIS Identification System user status must reapply. The gaining institution shall forward a new Request for Access to the AZAFIS System form to the AZAFIS Site Administrator.

- 1.5.5 Operators wishing to change their sign-in or password shall submit an updated AZAFIS Access form to the AZAFIS Site Administrator.

## **121.11 AUDITS OF AZAFIS IDENTIFICATION SYSTEMS**

- 1.1 The AZAFIS Site Administrator and DPS will annually audit the AZAFIS Identification Systems through electronic reports. These audit procedures are designed to assist in maintaining complete and accurate records and ensure that dissemination of information is made only to authorized individuals.
- 1.2 DPS documents all AZAFIS activity through the Department's contract as follows:
  - 1.2.1 Sagem Morpho for the Live Scan, Fast ID and OPPIS systems.
  - 1.2.2 ImageWare for the Mug Photo Interface Subsystem.
- 1.3 The AZAFIS Site Administrator shall maintain copies of all reports.

## **121.12 AZAFIS IDENTIFICATION SYSTEM USE, RESTRICTIONS AND VIOLATIONS**

- 1.1 Department use of the AZAFIS Identification Systems is restricted to:
  - 1.1.1 The administration of criminal justice system, such as the collection, storage and dissemination of criminal history records information, fingerprints and for identification purposes. Fingerprints shall be taken for official Department use only.
  - 1.1.2 Entering inmate photos and fingerprints into the AZAFIS Identification Systems.
  - 1.1.3 Providing Identification cards via the MPI system to inmates, volunteers, contractors and employees.
- 1.2 Department of Transportation, MVD files are accessible from the AZAFIS Identification System. Use of vehicle registration or drivers license information obtained from the AZAFIS Identification System is limited to law enforcement, criminal justice or MVD only. Any user that have access to the MVD database shall submit a written request that outlines the exact reasons for the inquiry and access. Access to any other database is strictly prohibited and may result in disciplinary action up to and including dismissal.
- 1.3 Misuse or fraudulent use of any AZAFIS Identification System may subject the violator to penalties outlined in Title 18, U.S. Code, Crimes and Criminal Procedure, and A.R.S 13-2316.
- 1.4 Data contained in the AZAFIS Identification System is documented criminal justice information and shall be protected to ensure correct, legal and efficient dissemination and use of information. This information is confidential and shall be handled accordingly. Any unauthorized request or receipt of information from AZAFIS Identification Systems may result in disciplinary action and/or criminal proceedings.
- 1.5 Staff shall report suspected violations of this Department Order, AZAFIS rules or regulations, or the misuse of the AZAFIS Identification Systems to the AZAFIS Site Administrator, who shall attempt to determine whether a violation or misuse occurred. Failure to report misuse may result in disciplinary action up to and including dismissal.

- 1.6 The AZAFIS Site Administrator shall:
- 1.6.1 Assist any Warden or Bureau Administrator in the follow-up investigation of any allegations of misuse involving the AZAFIS Identification System.
  - 1.6.2 Receive a copy of final reports of any such investigations.
  - 1.6.3 Contact DPS, FBI or other local, state or federal agencies whose confidential information may have been compromised or breached. Violators may be subject to Federal and State criminal proceedings.

**121.13 OPTICAL PRINT AND PHOTO IMAGE SUBSYSTEM (OPPIS)** – Through this database the Department may access all fingerprints and mug photos taken by any law enforcement agency within Arizona, since June 2002.

- 1.1 The OPPIS Subsystem is part of the AZAFIS Identification System and is maintained by DPS and the AZAFIS Site Administrator.
- 1.2 The OPPIS Operators shall adhere to the same guidelines and restrictions as any user of the AZAFIS Identification System, as outlined in section 121.12 of this Department Order.
- 1.3 OPPIS Operators are only authorized to print fingerprints and photos based on legitimate law enforcement requests. Any misuse of the system may result in disciplinary action up to and including dismissal as outlined in Section 121.12 of this Department Order.
- 1.4 OPPIS equipment shall be maintained in a secure environment with no inmate access and shall remain as a stand alone system, with only an operating system and OPPIS software.
- 1.5 Only photos are authorized to be emailed. Under no circumstances are fingerprints to be electronically sent or emailed. It is a violation of Federal and State law and this Department Order for fingerprints to be electronically disseminated. Violators may be subject to Federal and State criminal proceedings.

## DEFINITIONS

**ACCESS** - The National Crime Information Center (NCIC) Advisory Policy Board defines two types of access:

- Direct - Terminal access and dissemination within an agency.
- Indirect - Non-terminal access outside of an agency that has direct access.

**ACJIS LIAISON** - A staff member at each ACJIS site and each authorized work area, designated by the Deputy Director, Division Directors, Warden, Bureau Administrator, and the Contract Beds Operations Director, acting as the liaison between the work area and the SSO.

**ACJIS SYSTEM SECURITY OFFICER (SSO)** – A staff member who is the liaison between the Department of Public Safety and the ACJIS interface system contractor and ensures compliance with all laws, rules, regulations and this Department Order.

**ARIZONA AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM (AZAFIS)** – A computerized network which is controlled and housed by the Department of Public Safety (DPS).

**ARIZONA CRIME INFORMATION CENTER** - The Arizona counterpart of NCIC, available for entries and inquiries through the ACJIS network. The common acronym is ACIC. Most ACIC and NCIC files are totally independent.

**ARIZONA CRIMINAL JUSTICE INFORMATION SYSTEM** - A computerized network maintained by the Arizona Department of Public Safety (DPS) that is available to authorized local, state and federal criminal justice agencies. The ACJIS network is connected to two national computer networks, the National Law Enforcement Telecommunications System (NLETS) and the NCIC. ACJIS is available on a 24 hours per day, seven days per week basis.

**ARIZONA LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM** - A telecommunications system that provides for the exchange of criminal justice information between terminals within the State of Arizona. The common acronym is ALETS.

**AZAFIS SITE ADMINISTRATOR** – A staff member who is the liaison between the Department of Public Safety for the AZAFIS system and the vendors who provide the equipment and software for access to the AZAFIS Identification System.

**CONTROL TERMINAL AGENCY (CTA)** - A single state agency, under a shared management concept with the Federal Bureau of Investigation (FBI), which assumes responsibility as the control terminal (or main receiving point) for the state, through and by which users in the state access NCIC information. The CTA for the State of Arizona is the Department of Public Safety.

**CRIMINAL JUSTICE INFORMATION** - Information collected by criminal justice agencies that is needed for the performance of their legally authorized, required function. This includes persons (wanted, missing, unidentified), stolen property, criminal history record information, information compiled in the course of investigations of crimes that are known or believed on reasonable grounds to have occurred, including information on identifiable persons, and information on identifiable persons compiled in an effort to anticipate, prevent or monitor possible criminal activity.

**IDENTIFICATION OF SYSTEMS** – This Department Order establishes the use of technology in the positive identification of inmates and their criminal histories. The systems identified are:

- The Arizona Criminal Justice Information System (ACJIS)
- The Arizona Automated Fingerprint Identification System (AZAFIS)
- The Mug Photo Interface System (MPI)
- The electronic collection of ten print fingerprints (LIVE SCAN)
- The instant identification system for inmates (FAST ID)
- The system which allows access for printing all fingerprints taken and mug photos taken since June 2002 from the AZAFIS database (OPPIS)

**LIVE SCAN** – The equipment purchased by the Department, which allows the electronic capture of fingerprints. This equipment is directly connected to the Department of Public Safety database. This equipment and software allow the electronic sending of fingerprints to DPS for verification of identification.

**FAST ID** – This is equipment purchased by the Department, which allows the instant identification of an inmate by providing the name, date of birth, Arizona State Identification Number, sex, and if a DNA drawn has been completed on the individual. This equipment does not store or retain information. The two index fingerprints that are electronically sent to DPS for verification will be displayed within 60 seconds.

**MUG PHOTO INTERFACE SUBSYSTEM (MPI)** – This is software which allows the Department to interface with the AZAFIS system to take photos of inmates and store them in the statewide database. It also allows the department to access inmate photos when needed for law enforcement purposes.

**NATIONAL CRIME INFORMATION CENTER** - An FBI repository of files on persons and property. The common acronym is NCIC.

**NATIONAL LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM** - A message switching system for the interstate exchange of criminal justice information, also providing a variety of on-line help files. The common acronym is NLETS.

**OPTICAL PRINT AND PHOTO IMAGE SUBSYSTEM (OPPIS)** – This is software which allows the Department access to all fingerprints and mug photos taken by a law enforcement agency in the state of Arizona since June 2002.

**SECONDARY DISSEMINATION** - The dissemination of criminal justice information from an individual or agency that originally obtained the information from the central state repository, or through ACJIS, to another individual or agency authorized to receive the information.

{Original Signature on File}

---

Dora Schriro  
Director

#### **FORMS LIST**

- 121-1, Criminal History Information Request
- 121-2, ACJIS Secondary Dissemination Log
- 121-3, ACJIS Activity Log
- 121-4, ACJIS Teletype Message Log
- 121-5, Request for Access to Arizona Criminal Justice Information System
- 121-6, ACJIS Information Request List
- 121-7, Video and Department Order Viewing Log
- 121-8, AZAFIS Access Request

#### **AUTHORITY**

A.R.S. 13-2316, Computer Fraud, Classification.

A.R.S. 41-1750, Criminal Identification Section.

A.R.S. 41-2201 et. seq., Arizona Criminal Justice Information System.

28 C.F.R. 20.1 et. seq., Security and Privacy Regulations, Criminal Justice Information Systems.

18 U.S.C. 1030, Fraud and Related Activity in Connection with Computers