CHAPTER: 100

Agency Administration/Management

DEPARTMENT ORDER:

121 – Arizona Criminal Justice and Non-Criminal Justice Information And Identification System

OFFICE OF PRIMARY RESPONSIBILITY:

DIR

Arizona Department of Corrections

Department Order Manual

Effective Date:

June 27, 2014

Amendment:

N/A

Supersedes:

DO 121 (8/21/08)

Scheduled Review Date:

TBD

ACCESS

☐ **Contains Restricted Section(s)**

Charles L. Ryan, Director

TABLE OF CONTENTS

PURPOSE 1
RESPONSIBILITY 1
PROCEDURES 2
1.0 SYSTEM SECURITY OFFICER (SSO) 2
2.0 ACJIS LIAISONS 3
3.0 ACJIS OPERATOR CERTIFICATION 4
4.0 CRIMINAL JUSTICE PRACTITIONER 6
5.0 AUDITS 7
6.0 DOCUMENTATION 7
7.0 DISSEMINATION 9
8.0 APPLICATION OF INFORMATION 10
9.0 USE AND RESTRICTIONS 10
10.0 VIOLATIONS 11
11.0 ARIZONA AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM (AZAFIS/ADC) 11
12.0 AUDITS OF AZAFIS/ADC IDENTIFICATION SYSTEMS 14
13.0 AZAFIS/ADC IDENTIFICATION SYSTEM USE, RESTRICTIONS AND VIOLATIONS 14
14.0 OPTICAL PRINT AND PHOTO IMAGE SUBSYSTEM (OPPIS) 15
DEFINITIONS/GLOSSARY 15
FORMS LIST 15
AUTHORITY 16

PURPOSE

This Department Order establishes the use of the Arizona Criminal Justice Information System (ACJIS)—the Non-Criminal Justice Information and Identification System, the Mug Photo Interface Software (MPI), the Electronic Fingerprint Equipment (Live Scan), Fast ID, Paternity Deoxyribonucleic acid (DNA), and the 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 based on biometric fingerprint capture. This information shall be protected to ensure legal and efficient use. Employees operating any of the equipment and/or software shall be trained, tested, authorized, and/or certified. Employees reviewing any material displayed on these systems shall be trained in the processes and procedures of capturing biometric information and the legalities associated with the systems and laws governing the Arizona Automated Fingerprint Identification System (AZAFIS)/Department of Corrections (ADC) Identification System.

RESPONSIBILITY

Arizona Criminal Justice Information System (ACJIS) — The Deputy Director, Division Directors, Assistant Director, 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 Division Director for Prison Operations shall appoint a System Security Officer (SSO) for user security. The Chief Information Officer shall appoint a Local Agency Security Officer (LASO) for technical security.

ACJIS Operators, Criminal Justice Practitioners and the SSO are certified and approved by the Criminal Justice Information System (CJIS) — Control System Agency (CSA), 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:

- All ACJIS computers and printers are located in such a manner where only authorized personnel are able to read the monitor display and/or printed material. ACJIS computers may be placed in private prisons under contract with the Department for ADC ACJIS Operators only, and only after gaining authorization from the CSA.

- Computers and printers are located/secured in areas that only authorized personnel have access to. Manuals are located on-line for ACJIS Operator use.

- All changes regarding the equipment connected to the ACJIS network are coordinated with the CSA, through the SSO.

- Protection against unauthorized access is provided by appointing an ACJIS Liaison and ensuring employees with access to the ACJIS network information, whether directly or indirectly, are identified on an authorization list submitted to and maintained by the SSO.

Arizona Automated Fingerprint Identification System (AZAFIS) — The AZAFIS/ADC Site Administrator under the direction of the Offender Services Bureau Administrator shall be:

- Responsible for the oversight and operation of all AZAFIS/ADC Identification System(s), to include hardware, software, installation, and equipment maintenance (i.e., Electronic Fingerprint Equipment (Live Scan), MPI subsystem, Fast ID, DNA, and the OPPIS).

- The lead liaison between the Department and with DPS and shall coordinate the use of these systems with outside agencies and vendors. All changes regarding equipment connected to any of the AZAFIS/ADC Identification System shall be coordinated through the AZAFIS/ADC Site Administrator.

- Responsible for the verification of inmate fingerprints for positive identification upon admission to and release from the agency.

PROCEDURES

1.0 SYSTEM SECURITY OFFICER (SSO) – The SSO shall ensure the Department's staff accessing the ACJIS network is in compliance with all applicable laws, rules and regulations governing the use of ACJIS information. The SSO shall act as the liaison between the user agency and the CSA. All requests regarding the use of the ACJIS/National Crime Information Center (NCIC) system shall be coordinated through the SSO. The SSO shall:

1.1 Monitor system usage.

1.2 Enforce system discipline.

1.3 Ensure operating procedures are followed.

1.4 Serve as a central point within the Department for all ACJIS issues to include:

1.4.1 Record validations.

1.4.2 Quality control matters.

1.4.3 Security matters.

1.4.4 Agency personnel authorization/training/certification.

1.4.5 Maintaining a record of ACJIS Operators and Criminal Justice Practitioners.

1.4.6 Maintaining a Training Log which shall be kept on file for a six-month period coinciding with the semi-annual report to the CSA. Report periods are set by the CSA and are May 1st to October 31st and November 1st to April 30th.

1.4.7 Providing the CSA with updated lists of ACJIS Operators and Criminal Justice Practitioners as required and including them with the semi-annual report.

1.4.8 Ensuring ACJIS Operators and Criminal Justice Practitioners complete the necessary training as outlined in section 2.0 of this Department Order.

1.4.9 Processing requests for information/problems identified regarding ACJIS use.

1.4.10 Coordinating with the CSA all requests for information, training and updates.

1.5 Receive Monthly Statistical Reports from the CSA and route them to the appropriate ACJIS Liaison for review.

2.0 ACJIS LIAISONS – The ACJIS Liaison is usually the primary ACJIS Operator of the complex. At Central Office, it is a person assigned the duty of maintaining the ACJIS Criminal Justice Practitioner list for their division or work area. The ACJIS Liaisons shall:

2.1 Prepare and forward a list of authorized Criminal Justice Practitioners and ACJIS Operators to the SSO. This list shall be updated as changes occur.

2.2 Notify the SSO of any additions or deletions in personnel on the list as they occur.

2.3 Coordinate the training of prospective Criminal Justice Practitioners and ACJIS Operators.

2.4 Ensure employees requesting authorization as a Criminal Justice Practitioner or ACJIS Operator complete 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.

2.5 Ensure employees requesting authorization as a Criminal Justice Practitioner or ACJIS Operator complete the necessary training when they are first assigned to the position, and a review/refresher training every two years thereafter. Training consists of:

2.5.1 Viewing the "ACJIS Overview" DVD.

2.5.2 Completing the “CJIS On-Line” Security Awareness Training and reviewing this Department Order through sections 10.0. Access to the “CJIS On-Line” training is available from the SSO or local ACJIS Operator.

2.5.2.1 The Criminal Justice Practitioner or ACJIS Operator shall ensure the new Request for Access to ACJIS form is completed in full to include the training dates and all applicable signatures. This shall be completed every two years indicating the new training date.

2.6 Coordinate and schedule any ACJIS training with the CSA through the SSO.

2.7 Ensure employee training for Operator status take the on-line ACJIS Operator Training and Certification Test within six months from the date of the applicant's assignment to ACJIS related duties.

2.8 Re-certify ACJIS Operators every two years prior to their certification expiration date and ensure they complete refresher training as outlined in 2.7 of this section.

2.9 Maintain copies of ACJIS Operator certificates for audit purposes.

2.10 Share new/updated information with all ACJIS Operators as it is received from the SSO.

2.11 Monitor ACJIS usage by reviewing the Monthly Statistical Reports.

2.12 Enforce system discipline.

2.13 Advise the SSO and the chain of command regarding circumstances of non-compliance.

3.0 ACJIS OPERATOR CERTIFICATION

3.1 An employee requesting ACJIS Operator Certification shall:

3.1.1 Submit a Request for Access to ACJIS form through their chain of command to the appropriate ACJIS Liaison.

3.1.2 Complete the necessary training as outlined in section 2.0 of this Department Order.

3.1.3 Use the ACJIS solely for job-related purposes.

3.2 ACJIS Operator certifications are divided into the following four levels:

3.2.1 Level A – The on-line certification test consists of 50 questions. This level is for ACJIS Operators who enter records into the ACJIS, as well as modify, clear, cancel and/or locate records. These ACJIS Operators also interpret responses. Level "A" certification is limited to the SSO, a staff member who acts as a backup for the SSO, personnel assigned to the Central Office Communications Center, staff in the Fugitive Services Warrants and Hearings Unit, and the Sex Offender Coordination Unit.

3.2.2 Level B – The on-line certification test consists of 25 questions. This level is for ACJIS Operators who inquire into the ACJIS network and interpret responses. These individuals do not enter or update records.

3.2.3 Level C – Not applicable for the Department at this time. This level is for ACJIS Operators who use Mobile Digital Computers (MDC) only.

3.2.4 Level D – This on-line certification test consists of ten questions. This level is for agency Information Technology personnel who work with the ACJIS Interface System.

3.3 Prior to approving the request, the SSO shall conduct a current criminal history check and send a request to the Background Investigations Unit to ensure a fingerprint card has been submitted to DPS. The SSO shall notify the CSA, in writing, of any record located.

3.3.1 If a record of any kind is found, the SSO shall deny access pending review of the record in coordination with the CSA.

3.3.2 If the SSO and/or the CSA determine access is not in the public interest, such access shall be denied and the requesting authority shall be notified, in writing, of the denial.

3.4 If approved, the ACJIS Operator shall be assigned a certification number by the CSA, through the SSO. The SSO shall add the ACJIS Operator to the Department's ACJIS Interface System and notify the ACJIS Operator of the information necessary to access the system.

3.4.1 The ACJIS Operators shall train for a period, not to exceed six months, during which time they routinely perform ACJIS operations with supervisory monitoring. The certification test may be taken at any time during the six month period.

3.5 The ACJIS Operator tests are conducted on-line, and located at a restricted site that is accessible by ACJIS Operators holding a current, active Terminal Operators Certification number issued by the CSA. ACJIS Operators are allowed to use only the ACJIS Operating Manual, which is also on-line during the test. Tests shall be administered on an individual basis only. Group testing or polling of answers is prohibited. At this time, there is no time limit on the test; however, it shall be completed in one sitting.

3.6 ACJIS Operators are expected to know their certification number and keep it secure. Certification numbers remain on file with the CSA and are not re-assigned.

3.7 Certifications are valid for two years from the date of issue. Re-certification is required prior to the expiration date on the certificate.

3.7.1 The ACJIS Test System scores the test immediately. At the end of the test, ACJIS Operators who pass are given an option to print out their certificates. ACJIS Operators, who fail the re-certification test, shall wait 24 hours before they can re-test.

3.7.2 ACJIS Operators whose certification has expired are not authorized to operate ACJIS computers.

3.7.3 ACJIS Operators who do not wish to re-certify 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 CSA and shall be deleted from the Department's ACJIS Interface System by the SSO.

3.8 An ACJIS Operator who does not test by the expiration date shall be locked out of the ACJIS by the CSA. The ACJIS Operator shall contact the SSO who shall request, the CSA to re-activate their Terminal Operators Certification number. The re-activation shall only be good until the Monday following the re-activation date. If the test is still not completed, the ACJIS Operator shall be locked out again. If an extension of the date is needed, the SSO shall submit a written request prior to the expiration date, to include a reason for the extension to the CSA.

3.9 ACJIS Operators transferring to a different position in the Department who wish to retain their certification shall contact the gaining ACJIS Liaison.

3.9.1 Only when the transfer is into a position requiring ACJIS access shall the ACJIS Operator be allowed to maintain certification.

3.9.2 The gaining ACJIS Liaison shall forward a new Request for Access to ACJIS form to the SSO.

3.10 An ACJIS Operator, who has transferred into a position which requires requesting and viewing ACJIS information without having access to an ACJIS computer, shall be downgraded to a Criminal Justice Practitioner. The employee shall contact the gaining ACJIS Liaison, who shall notify the SSO.

3.10.1 The gaining ACJIS Liaison shall forward a new Request for Access to ACJIS form to the SSO indicating a change of status.

3.10.2 The Operator certification number shall be placed on inactive status by the CSA and the ACJIS Operator deleted from the Department's ACJIS Interface System by the SSO.

3.11 The ACJIS Operators who have been placed on inactive status shall contact the ACJIS Liaison to request authorization to return to active status.

3.11.1 Inactive ACJIS Operators, who request to be placed back on active status, are not required to re-test or re-certify unless the certification has expired or the level of certification is higher than the previous level held.

3.11.2 The ACJIS Liaison shall notify the SSO when an ACJIS Operator is returned to active status.

3.12 ACJIS Operators who:

3.12.1 Request to upgrade their certification level shall complete a new Request for Access to ACJIS form. The SSO shall notify the CSA to upgrade the access in the ACJIS. Once this is completed, the ACJIS Operator shall take the on-line test for the desired level.

3.12.2 Request to downgrade their certification level do not need to take an additional exam, but shall notify the SSO, through their ACJIS Liaison, in writing of their intention. A new Request for Access to ACJIS form shall be completed indicating the lower certification level.

3.13 ACJIS Operators who change their name shall submit an updated Request for Access to ACJIS form to the SSO through their ACJIS Liaison.

4.0 CRIMINAL JUSTICE PRACTITIONER

4.1 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.

4.2 The employee shall complete and submit a Request for Access to ACJIS form, through the chain of command to the appropriate ACJIS Liaison. The ACJIS Liaison shall ensure the employee completes the necessary training as outlined in section 2.0 of this Department Order. Then forward the forms to the SSO who shall approve or deny it.

4.3 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.

4.3.1 The position shall require ACJIS access in order for the Criminal Justice Practitioner to retain their status.

4.3.2 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.

4.3.3 The ACJIS Liaison at the new location shall forward a new Request for Access to ACJIS form to the SSO.

4.4 Criminal Justice Practitioners who change their name shall submit an updated Request for Access to ACJIS form to the SSO, through their ACJIS Liaison.

5.0 AUDITS

5.1 ACJIS sites are routinely audited every three years by the CSA. Audit procedures are designed to assist in maintaining complete and accurate records and ensure dissemination of information is made only to authorized individuals.

5.2 A direct audit is an administrative review triggered as a result of an incident or allegation of possible misuse of the system or information. An administrative review by the CSA is designed to detect, process issues which may result in noncompliant action by the ACJIS site.

5.3 If compliance issues are detected, the CSA shall do a report and submit the report to the Director and the SSO containing recommendations and/or specific requests in order to bring the Department and/or ACJIS site into compliance.

5.4 The SSO shall ensure the audit findings and/or corrective actions are disseminated through the chain of command to the appropriate executive staff member and the Director.

6.0 DOCUMENTATION

6.1 All ACJIS activity shall be logged on an automated log within the Justice Web Interface System. The Justice Web Interface is the Interface System used by the Department.

6.1.1 ACJIS activity may be documented manually on the ACJIS Activity Log, Form 121-3; however, this is not absolutely necessary due to the automated logging with the Justice Web Interface.

6.1.2 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.

6.1.3 Secondary dissemination of ACJIS information by a Criminal Justice Agency shall be documented on the ACJIS Secondary Dissemination Log, Form 121-2 and retained for one year. ACJIS information can only be secondarily disseminated by an authorized Criminal Justice Agency person to another authorized Criminal Justice recipient.

6.1.3.1 Secondary dissemination of ACJIS information by a Non-Criminal Justice Agency (NCJA) to any other agency, company, or person, is not authorized by Arizona Revised Statute (A.R.S.) §41-1750.

6.2 Requests for ACJIS information shall be submitted on a Criminal History Information Request, Form 121-1, signed by the Criminal Justice Practitioner making the request, or on other approved written source such as a visitation form or the ACJIS Information Request List, Form 121-6.

6.2.1 The purpose of a request shall be obtained from the requestor prior to accessing the ACJIS network. Requests shall be for criminal justice purposes. Curiosity checks are prohibited.

6.2.2 Telephone requests for information are not authorized. A Criminal History Information Request may be transmitted by facsimile (FAX) or scanned/emailed to the ACJIS Operator.

6.2.3 Requests via e-mail may be accepted providing they are sent by an authorized practitioner and comes from within the Department domain. The email shall include the same information as the Criminal History Information form, including name, date of birth, and the reason for the request. Additional information such as race, sex, social security number is helpful, but optional.

6.3 The ACJIS Operator's response to a request for information shall be documented on the Criminal History Information Request form or on other approved documents as stated above.

6.4 ACJIS Operators at all Central Office and Institution ACJIS offices shall maintain copies of information requests and Criminal History Information Requests forms outlined in this section for a three year period (coinciding with the audit time period).

6.4.1 Print-outs/reports from the ACJIS network shall not be filed or maintained inside the secure perimeter of a unit.

6.4.1.1 In private prisons under contract with the Department, ACJIS printouts are to be maintained and filed in the ADC ACJIS office where applicable.

6.4.2 Print-outs/reports may be taken to a secured/restricted office which is located inside a unit, provided they are kept secured and out of sight of unauthorized persons, to include inmates and unauthorized staff.

6.4.3 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. They shall be destroyed as outlined in 6.5 of this section.

6.4.4 Reports of criminal history record information, obtained from the ACJIS network, shall never be maintained in any inmate record/file. (Printouts of wanted persons queries are not considered criminal history information and may be maintained in an inmate record/file.)

6.4.5 Printouts of identifying information shall be attached to outstanding wanted persons for identification purposes.

6.5 Approved methods for the destruction of printed documents obtained from the ACJIS network are:

6.5.1 Shredding — the preferred method of destruction. The shredded material shall be disposed of properly.

6.5.2 Burning — shall only be used where it is legal and when it can be safely monitored and contained.

7.0 DISSEMINATION

7.1 The existence or absence of criminal history information shall not be confirmed to any individual or agency not authorized to receive the actual information. Authorized individuals are those who are authorized criminal justice practitioners or certified operators with the Department. Authorized agencies are agencies that hold an active Originating Agency Identifier (ORI) issued by the FBI.

7.2 Employees who are not authorized or approved shall not have access, whether directly or indirectly, to information obtained from the ACJIS network.

7.3 It is incumbent upon the Department to ensure dissemination of information is made, directly or indirectly, only to authorize personnel. Authorized personnel are those who have completed the training and paperwork necessary for all Criminal Justice Practitioners. Any departure from this requirement warrants the removal of the ACJIS Operator from further access to the ACJIS network or information.

7.4 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.

7.5 Secondary dissemination of information to another agency or department shall be documented in accordance with section 6.0 of this Department Order. The Originating Agency Identifier (ORI) of the requesting agency/department shall be used when accessing the ACJIS network for secondary dissemination.

7.5.1 Secondary dissemination of information by Non-Criminal Justice Agencies, which for the Department is the Contract Beds Bureau, to other agencies or companies is prohibited unless specifically authorized by law.

7.6 Each employee who has access to ACJIS information shall be identified on an authorization list.

7.6.1 This list is maintained by the SSO and the CSA, and shall contain the individual's name, date of birth, date of hire and, if applicable, the Operator's certification number. Additional information may include the individual's work location, the date the ACJIS training was completed and the expiration date.

7.6.2 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.

7.7 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 (i.e., riot, hostage, and escape).

8.0 APPLICATION OF INFORMATION

8.1 ACJIS information shall be reviewed to determine a positive or negative response to the inquiry.

8.1.1 A negative response will not indicate that the person or property inquired upon is not wanted; missing or stolen, or no criminal history record information exists.

8.1.2 The receiving party shall use neither a positive or negative response as the sole basis for decision-making.

8.2 Name-only searches, unsupported 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 the Background Investigations Unit, or the SSO with a Criminal History Information Request for technical comparison.

9.0 USE AND RESTRICTIONS

9.1 The Department shall use the ACJIS network only for the following:

9.1.1 The administration of criminal justice, i.e., the collection, storage and dissemination of criminal history record information.

9.1.2 Entering and maintaining the wanted person's entries for parolees on Parole Absconder or Home Arrest Curfew Violator status; the Convicted Persons on Supervised Release (CPSR); Deported Felon status for the half to Deport Releases, and the sex offender registration entries entered by the Sex Offender Unit.

9.1.3 Conducting background investigations on prospective employees, visitors, volunteers, contractors, vendors, or anyone who wants to access the secure perimeter of an institution or complex.

9.2 The Contract Beds Bureau, as a Non-Criminal Justice Agency, uses the ACJIS network for security clearance processing of all persons requesting access to Non-Criminal Justice Facilities (NCJ).

9.3 Any Criminal Justice Agency, which obtains criminal history information from the CSA 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 CSA or from the originating agency.

9.3.1 The Contract Beds Bureau assumes responsibility for the security of any criminal history information obtained from the CSA or through ACJIS, and shall not secondarily disseminate this information to any individual, agency or company not authorized to receive this information.

9.4 The Background Investigations Unit shall process all background investigations of prospective employees, volunteers and contractors of the Department as outlined in Department Order #204, Volunteer Services, Department Order #205, Contractor Security, and Department Order #602, Background Investigations.

9.5 The Department of Transportation Motor Vehicle Division files are accessible from the ACJIS network. Use of vehicle registration or driver's license information, obtained from the ACJIS network, is limited to law enforcement, criminal justice, or Motor Vehicle Division purposes only. Curiosity inquiries are forbidden.

10.0 VIOLATIONS

10.1 Computer misuse or fraudulent use may subject a violator to the penalties outlined in U.S. Code Title 18 - Crimes and Criminal Procedure; A.R.S. §13-2316 - Computer Tampering; A.R.S. §28-455 - Release of Information and A.R.S. §41-1756 - Unauthorized Access to Criminal History. Utilization of state computers or other devices shall be in accordance with Department Order #102, Information Technology.

10.2 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 in nature and shall be treated accordingly. Any unauthorized request and/or receipt of ACJIS/NCIC material may result in criminal proceedings.

10.2.1 Staff shall report suspected violations of this Department Order, ACJIS rules or regulations, or misuse of the ACJIS network to the SSO, who shall determine whether a violation or misuse has occurred.

10.2.2 An employee who is not authorized/approved shall not have direct or indirect access to information obtained from the ACJIS network.

10.3 The SSO shall provide assistance to Wardens or Bureau Administrators investigating allegations of improper use of the ACJIS. A copy of the final reports shall be forwarded to the SSO for the purpose of follow-up with the CSA and/or the FBI/NCIC audit team, if necessary.

11.0 ARIZONA AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM (AZAFIS/ADC)

11.1 All AZAFIS/ADC Identification System equipment shall be located in a secured and locked area within the prison complex/Central Office and site positioned in such a manner that only authorized personnel can have clear access to the equipment and operating manuals. The only Central Office sites, authorized to house investigative (search and print only) MPI systems, are the Central Office Communication Center, the Inspector General's Bureau, the Recruitment Unit for Selection and Hiring, the AZAFIS/ADC Site Administrator and Community Corrections Bureau.

11.1.1 The AZAFIS/ADC Identification System includes Live Scan for the capture of both 10-print and palm prints, the MPI, Fast ID, the OPPIS, DNA, database desktop system. For specific information regarding the AZAFIS/ADC Identification System operation and process, refer to Department Order #901, Inmate Records Information and Court Action.

11.2 The AZAFIS/ADC Site Administrator shall:

11.2.1 Ensure only authorized staff have access to the AZAFIS/ADC Identification Systems.

11.2.2 All authorized users of the system are to abide by all state statutes, rules and regulations governing the use of the equipment and information received from the system.

11.2.3 Maintain and update a master record log of all three categories of AZAFIS/ADC Identification System Users and Officers and notify DPS when staff are no longer authorized to access the system.

11.2.3.1 The three separate AZAFIS/ADC Identification System User Categories are as follows:

11.2.3.1.1 Full User – These are users that shall be granted full access to all rights for the full MPI system. Primarily, they shall be Criminal Investigations Unit investigators and key investigation staff who have met the requirements and passed the appropriate testing and taken yearly refresher exams.

11.2.3.1.2 Authorized Users/Identification System Officers – These are users assigned to perform 10-print fingerprint captures, mug photo captures and Fast ID operations, take DNA samples and Paternity DNA samples. They must have taken and passed a yearly refresher exam and have hands-on training.

11.2.3.1.3 Administrative Users – These are users, who are identified by Wardens as key administrators, who shall know the basic operation of Fast ID and how to locate and print a photo from MPI. They must have taken and passed a yearly refresher exam and have hands-on training.

11.2.4 Provide all AZAFIS/ADC Identification System Officers and Users with training, as deemed appropriate.

11.2.5 Maintain quality control use of the systems by auditing monthly reports provided by the vendors. Disseminate all notices and information regarding the AZAFIS/ADC Identification System and provide authorization and training for all AZAFIS/ADC Identification System Users and Officers.

11.2.6 Process requests for information and problems with the systems in a timely manner.

11.2.7 Coordinate with DPS and appropriate vendors all requests for information, training and updates.

11.2.8 Ensure vendors supply Monthly Statistical Reports and notify of any and all routine problems.

11.3 The Deputy Warden of Operations, or designee, for each institution shall:

11.3.1 Maintain a log of all active AZAFIS/ADC Identification System Officers/User, which shall include the employee's name, shift and Employee Identification Number (EIN), the date the employee was assigned to use the AZAFIS/ADC Identification System and in which the date the employee's authorization was suspended or removed.

11.3.2 Notify the AZAFIS/ADC Site Administrator of any changes in personnel, to include staff members who are no longer authorized to access the system, within ten workdays of the changes.

11.3.3 Coordinate through the AZAFIS/ADC Site Administrator, the scheduling of the AZAFIS/ADC Identification System Authorized Officers.

11.3.4 Coordinate the training of the AZAFIS/ADC Identification System Officers at annual conferences, mandatory annual on-line training and seminars.

11.3.5 Ensure staff, requesting authorization to use any AZAFIS/ADC Identification System, complete and submit the AZAFIS Access Request, Form 121-8, to the AZAFIS/ADC Site Administrator and provide proof of passing the required training.

11.3.6 Delay decisions regarding the implementation of new hardware or software or contact any vendor or DPS for assistance until authorization is received from the AZAFIS/ADC Site Administrator or designee.

11.3.7 Forward all requests regarding AZAFIS/ADC Identification System hardware, or software issues to the AZAFIS/ADC Site Administrator for determination and action.

11.4 AZAFIS/ADC Identification System employees, requesting to be an AZAFIS/ADC Identification System User and Officer, shall:

11.4.1 Have a bona fide job-related assignment.

11.4.2 Complete, sign and submit a current AZAFIS Access Request form through their chain of command to the AZAFIS ADC Site Administrator for approval.

11.4.3 Take and pass authorized yearly refresher training by DPS and the AZAFIS/ADC Site Administrator, prior to operating the AZAFIS/ADC Identification System.

11.4.4 Complete, if approved by the AZAFIS/ADC Site Administrator, and the unit Administrator, two weeks of on the job training from an AZAFIS/ADC Identification System Officer, who has a minimum of one-year experience or has been approved by the AZAFIS/ADC Site Administrator.

11.4.5 AZAFIS/ADC Identification System Users/Officers:

11.4.5.1 Whom have forgotten their sign-on or passwords shall contact the AZAFIS/ADC Site Administrator for assistance. At no time shall an AZAFIS/ADC Identification System User/Officer directly contact DPS. If a User/Officer repeatedly cannot remember their sign-on and password, the AZAFIS/ADC Site Administrator has the right to deny their access.

11.4.5.2 Shall have transferred to a different position within the Department and wish to retain their AZAFIS/ADC Identification System User status shall reapply. The gaining institution shall forward a new AZAFIS Access Request form to the AZAFIS/ADC Site Administrator.

11.4.5.3 Shall use an assigned sign-on password and not share passwords with any other staff or AZAFIS/ADC Identification System User or Officer.

12.0 AUDITS OF AZAFIS/ADC IDENTIFICATION SYSTEMS

12.1 The AZAFIS/ADC Site Administrator and the Arizona State AZAFIS Site Administrator (DPS designated employee) shall annually audit the AZAFIS/ADC Identification Systems through electronic reports. These audit procedures are designed to assist in maintaining complete and accurate records and ensure dissemination of information is made only to authorized individuals.

12.2 Department of Public Safety documents all AZAFIS/ADC Identification System activity through the Department's contract (i.e., as Morpho - Trak for the Live Scan, Fast ID and OPPIS systems). The AZAFIS/ADC Site Administrator shall maintain copies of all reports.

13.0 AZAFIS/ADC IDENTIFICATION SYSTEM USE, RESTRICTIONS AND VIOLATIONS

13.1 Department use of the AZAFIS/ADC Identification Systems is restricted to the administration of the criminal justice system, such as:

13.1.1 The collection, storage and dissemination of criminal history records information, fingerprints and photos for identification purposes. (Fingerprints shall be taken for official Department use only).

13.1.2 Entering inmate photos and fingerprints into the AZAFIS/ADC Identification System.

13.1.3 Providing Identification cards, via the MPI system, to inmates, volunteers, contractors and employees.

13.1.3.1 At no time should any photo of a Department employee be used anything other than for the issuance of an Identification card or replacement card, unless written permission is granted by the Offender Services Bureau Administrator or his/her designee.

13.2 At no time should fingerprints be taken by any Department Authorized User for any other purpose than Department business.

13.3 Only authorized Full Users of the AZAFIS/ADC Identification System are afforded the access to the Department of Transportation Motor Vehicle Division files via the AZAFIS Identification System. Use of vehicle registration or driver's license information, obtained from the AZAFIS Identification System, is limited to law enforcement, criminal justice or Motor Vehicle Division personnel only.

13.4 Misuse or fraudulent use of any AZAFIS/ADC 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.

13.5 Data contained in the AZAFIS/ADC 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/ADC Identification Systems may result in the immediate denial of access to the system, disciplinary action, and/or criminal proceedings.

13.6 Staff shall report suspected violations of this Department Order, AZAFIS/ADC rules or regulations, or the misuse of the AZAFIS/ADC Identification Systems to the AZAFIS/ADC Site Administrator, who shall attempt to determine whether a violation or misuse occurred and work in cooperation with the complex Administration to reach a final resolution. Failure to report misuse may result in disciplinary action up to and including dismissal.

13.7 The AZAFIS/ADC Site Administrator shall:

13.7.1 Assist any Warden, Administrator or Bureau Administrator in the follow-up investigation of allegations of misuse involving the AZAFIS/ADC Identification System.

13.7.2 Receive a copy of final reports of investigations.

13.7.3 Contact DPS, the FBI or any 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.

14.0 OPTICAL PRINT AND PHOTO IMAGE SUBSYSTEM (OPPIS)

14.1 The OPPIS Subsystem is part of the AZAFIS/ADC Identification System and is maintained by DPS and the AZAFIS/ADC Site Administrator.

14.2 The OPPIS Operators shall adhere to the same guidelines and restrictions as any AZAFIS/ADC Identification User and Officer of the AZAFIS Identification System, as outlined in section 13.0 of this Department Order.

14.3 The 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 13.0 of this Department Order.

14.4 The OPPIS equipment shall be maintained in a secure environment within the Offender Services Bureau Administration Central Office site, with no inmate access, and shall remain as a stand-alone system with only operating system and OPPIS software.

14.5 Only photos are authorized to be 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/GLOSSARY

Refer to the Glossary of Terms

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 (ACJIS)
121-6, ACJIS Information Request List

121-8, AZAFIS Access Request

AUTHORITY

A.R.S. §13-2316, Computer Fraud, Classification
A.R.S. §28-455, Release of Information
A.R.S. §41-1750, Criminal Identification Section
A.R.S. §41-1756, Unauthorized Access to Criminal History
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