Arizona Department of Public Safety
Criminal Justice Services Bureau
Access Integrity Unit

Arizona Noncriminal Justice Compliance Program

Noncriminal Justice Agency Guide for Fee-Based State and Federal Criminal History Checks

ABBREVIATED GUIDE FOR PUBLIC RELEASE

Document Date: May 2021

Table of Contents

Summary of Changes

12/2020	• *Contact List information for Applicant Team, AIU Supervisor, NCJ Team* • *1.3 User Agreement* • *2.5 FBI Notification of Applicant Privacy Rights and Privacy Act Statement of 1974* • *2.7 Required Information on Each Fingerprint Card* • *2.8 Example Fingerprint Cards* • *2.9 Inventory Sheets* • *2.10 Payment and Submission Packets* • *2.11 Rejected Fingerprint Cards/Resubmissions* • *2.12 State Results* • *2.13 FBI Results* • *3.2 Applicant Process* • *4.1.1 Information Changes* • *4.1.2 Authorized Personnel List* • *4.2.1 Required Training for Authorized Personnel* • *Acronym Glossary* • *Appendix B* • *Appendix D*

Introduction

This guide was created to assist Arizona agencies which submit fingerprints and receive criminal justice information (CJI) and criminal history record information (CHRI) for noncriminal justice purposes pursuant to authorizations allowed by state and federal law.

Passed by Congress in October 1972, Public Law 92-544, provided for funds to be allocated for the exchange of criminal history identification records for noncriminal justice purposes, pursuant to approved statutes. In 1998, the National Crime Prevention and Privacy Compact (Compact) Act was passed allowing signatory states to exchange criminal history records for noncriminal justice purposes according to a uniform standard. The 1998 act also established the National Crime Prevention and Privacy Compact Council to regulate and assist in maintaining a method of exchange of criminal history record information which protects both public safety and individual privacy rights. The Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Division houses the largest repository of fingerprint criminal history records and is charged with the responsibility and authority to oversee the exchange of such records. Federal laws, regulations, and policies have been formed both to govern the release of information exchanged through the FBI and to require states to regulate access, use, quality, and dissemination of state-held records.

Arizona Revised Statute (A.R.S.) § 41-1750 delineates the responsibilities of the CJIS Systems Agency (CSA), the central state repository, and the authorized receiving organizations. The Arizona Department of Public Safety (AZDPS) is the CSA for Arizona and operates the central state repository which collects, maintains, and disseminates criminal history in Arizona. A.R.S. § 41-1750 also provides state authorizations for the dissemination of criminal justice information and criminal history record information for noncriminal justice purposes. Additional authorizations may be found in Arizona statutes, executive orders, and under applicable federal laws.

Both state and federal criminal justice and criminal history record information is subject to laws, rules, and regulations governing its access, use, handling, and dissemination. This guide is intended to assist noncriminal justice agencies with proper fingerprint submittals, guide agencies' responsibilities for appropriate information handling, and inform agencies of requirements associated with the use of the state and federal criminal history check process.

Arizona Department of Public Safety
Contact List

Fingerprint Submissions for Criminal History Checks

Department: Applicant Team

The Applicant Team handles fingerprint submissions, inventory sheets, receipt of payment, and distributes the CHRI to agencies. Available Monday through Friday from 8:00 a.m. to 5:00 p.m. Closed on state and federal holidays.

Applicant Team
Phone: (602) 223-2223
Fax: (602) 223-2972

Arizona Department of Public Safety Applicant Team P.O. Box 18430 | Mail Drop 3190 Phoenix, AZ 85005-8430	Supervisor: Ms. Zelma Jones Phone: (602) 223-2722 E-mail: ZJones@azdps.gov

Administrative & Compliance: Audits, Training, and Privacy & Security

Department: Access Integrity Unit (AIU)

The Access Integrity Unit handles agency access requests, program compliance, training, privacy & security, policies & procedures, and operational compliance audits. The AIU is also the liaison between criminal justice and noncriminal justice agencies and the FBI for initial legal authorization approval & subsequent changes. Available Monday through Friday from 8:00 a.m. to 5:00 p.m. Closed on state and federal holidays.

Noncriminal Justice Compliance Team
ACJIS Compliance Specialists/Instructors: Ms. Lisa Tarr and Mr. Stephen Skuba Jr.
Phone: (602) 223-2488
E-mail: NCJA@azdps.gov
Fax: (602) 223-2926
Website: www.azdps.gov/services/government/ncj

Arizona Department of Public Safety Access Integrity Unit ATTN: Noncriminal Justice Compliance P.O. Box 6638 | Mail Drop 3160 Phoenix, AZ 85005-6638	Supervisor: Ms. Veronica Luna Phone: (602) 223-2580 Email: VLuna@azdps.gov

Section 1 – General Overview

1.1 AZDPS Overview

The AZDPS houses the Central State Repository (CSR) and is the state agency responsible for collecting, maintaining, and disseminating criminal history records in Arizona. AZDPS is also the National Crime Information Center (NCIC) CJIS Systems Agency (CSA) for Arizona and manages the Arizona Criminal Justice Information System (ACJIS). ACJIS is the state's criminal justice information system that provides authorized Arizona agencies with various types of record information such as criminal history records, sex offender registration information, and wanted persons information.

An executive officer is designated as the CJIS Systems Officer (CSO) to ensure that information stored at the CSA/CSR is accurate and complete. The CSO and CSA responsibilities include:

- Monitoring agencies in the state to ensure system maintenance and records security.
- Ensuring proper dissemination of criminal justice information, including criminal history record information.

Established policies, procedures, and standards must be strictly adhered to maintain the integrity of the system and its records. Within AZDPS, the Access Integrity Unit (AIU) performs several duties regarding compliance with the federal and state regulations for system access and maintenance:

- Conducting audits of the use and dissemination of ACJIS, NCIC, and criminal history records.
- Training concerning the use of system information.
- Monitoring system access and researching/investigating security breaches.

The Noncriminal Justice Compliance Team is a part of the AIU.

The AZDPS Applicant Team processes the fingerprint cards, associated payments, and returns the criminal history check results to the submitting agency via mail or electronic results, depending on the method of submission.

1.2 Authorizations and Access

Each noncriminal justice access must be authorized by a specific state statute, city, county, or town ordinance, executive order, federal law, or tribal resolution. Agencies that desire to open new access to submit fingerprints must apply with the AZDPS.

1.2.1 Application for Access

Before submitting fingerprint cards and receiving criminal history information, a new user agency must:

- Complete an application for access,
- Sign a Noncriminal Justice User Agreement,
- Submit to a site inspection,
- Attend an Initial Access & NCJ Compliance Training, and
- Submit an authorized personnel list.

Non-profit agencies must also submit a Non-Profit Declaration Form and by law are only eligible to receive Arizona criminal history record information. For the application to be approved,

agencies must provide an applicable legal authorization in place to open access; the authorization must be cited on the application. Applications are available for download on the AZDPS website at www.azdps.gov/services/government/ncj in the "Applying for Access" tab. Applications are reviewed by the AZDPS AIU. If approved, AIU will supply a user agreement and information regarding the additional steps to be completed to establish access.

New agencies must also attend an Initial Access & NCJ Compliance Traininghosted by the AZDPS. The training is designed to assist agencies in carrying out its responsibilities under the user agreement and maintaining compliance with applicable laws and regulations. Once initial requirements are met, the agency is issued an Originating Agency Identifier (OCA), which is a nine-character alphanumeric identifier beginning with "XX"; this number is the agency's submission access number for fingerprint-based criminal history record checks. Fingerprint cards and inventory sheets are provided by the AZDPS free of charge.

1.2.2 New Authorizations/Changes to Authorizations

New authorizations (such as new city/town/county ordinances, or Tribal Resolutions, etc.) must be submitted to the AZDPS for approval prior to the submission of fingerprints for the new purpose will be processed. If the fingerprints will be used to check both state and FBI records, then the AZDPS will also submit the authorization to the FBI for approval. The AZDPS can assist agencies with ensuring the proper requirements are included in new/revised authorizations to obtain approval from the FBI.

If there are any changes to an already approved authorization, the changes must be resubmitted to the AIU for approval from the FBI (i.e., the authorization is a city ordinance and that ordinance is later superseded), and must still include the necessary language allowing for the submission of fingerprints/receipt of the criminal history record information. An agency may have their access suspended if changes to their authorization do not include the necessary requirements.

1.2.3 Criminal Justice versus Noncriminal Justice Accesses

Some agencies have both Criminal Justice & Noncriminal Justice access to criminal history record information. Criminal justice agencies are **not** permitted to use their criminal justice access (terminal and non-terminal) for noncriminal justice purposes. Noncriminal justice purposes include but are not limited to licensing determinations, noncriminal justice employment/volunteers, adoptions, guardianships, conservators, etc.

Fingerprint cards or electronic fingerprints must be submitted to the AZDPS Applicant Team with a noncriminal justice OCA to obtain criminal history checks for noncriminal justice purposes; "running" III checks are not permitted. The use of CHRI obtained from noncriminal justice fingerprints is strictly limited to the noncriminal justice purpose and **may not** be shared for criminal justice purposes. For questions regardingcriminal justice and noncriminal justice purposes, please contact the AIU.

1.3 User Agreement

Each agency authorized to receive CJICHRI must sign a user agreement. The user agreement is a contractual agreement between the authorized receiving organization and AZDPS; it must be signed by both the Arizona CSO and the appropriate authority at the user agency. The appropriate authority is any individual authorized to enter into a legal agreement between an

agency and the AZDPS. This includes Agency Heads, referred to by AZDPS as the CEO, an Agency Security Contact (ASC), and/or anyone else at an agency that is designated to be an authorized signor. The signor is only required to be on the Authorized Personnel List (APL) if they have access to criminal history record information.

The user agreement contains Terms and Conditions which include the following:

- Authority and Purpose: The user agreement states the nature of the requesting organization, the purpose for which criminal justice information and/or criminal history is requested, and the specific legal authorization granting access to the information.

  A.R.S. § 41-1756 states that it is a class 6 felony for any person who commits unauthorized access to criminal history record information.

- Sanctions/Penalties: The user agreement is subject to cancellation by either party with 30 days written notice. AZDPS reserves the right to suspend service for violations or investigations of apparent/alleged violations of the user agreement. State and federal civil and/or criminal penalties may apply for misuse of CJI/CHRI.

- Agency Security Contact: The user agreement requires the appointment of an Agency Security Contact (ASC) to act as liaison with AZDPS. The responsibilities of the ASC are covered in Section 4.

- Training: Agencies are responsible for mandatory training requirements. New agencies opening fingerprint access must attend Initial Access & NCJ Compliance Training in-person or online before submitting fingerprint cards. Existing agencies are not required to attend training at DPS but are welcome to do so for refresher training or with the appointment of a new Agency Security Contact. All agency personnel who view or handle CHRI must complete the standard online training (currently called CJIS Online) and undergo agency internal training on CHRI security and handling based on the required policies/procedures.

- Policies/Procedures: As part of privacy and security, agencies must implement policies and procedures which provide for the security and proper handling of the CJI/CHRI. Agencies should also have rules for fingerprint submissions which include proper applicant identification and protecting the fingerprint card from tampering.

Section 2 – Fingerprint Submissions & Results

The information in this section is intended to assist agencies with the following:

- Understanding the different types of fingerprinting programs in Arizona.
- Using quality assurance procedures for applicant identity verification and fingerprint card tampering prevention.
- Compliance with FBI applicant privacy notification requirements.
- Properly filling out the fingerprint card and inventory sheet.
- Assembling a fingerprint submission packet, including appropriate payment.
- Interpreting state and FBI results.

2.1 Arizona Fingerprint/Fee-Based Criminal History Record Check Programs

Two different fingerprinting programs in Arizona involve the use of a person's official criminal history record information: the Fingerprint Clearance Card process and the Noncriminal Justice (NCJ) Fingerprint Criminal History Check process. The subsections below explain the difference between the two processes. Please note that this guide concentrates on fingerprint submissions and compliance rules for the NCJ Fingerprint Criminal History Check process. Applicant fees apply to both programs.

2.1.1 Fingerprint Clearance Card Program

The Fingerprint Clearance Card process occurs between an individual applicant and AZDPS, not an agency. To apply for a fingerprint clearance card, the individual MUST fall into one of the categories listed on either the Identify-Verified Prints (IVP) or the non-IVP clearance card application; if the individual does not fit into one of the categories, then the person is not eligible to apply, and there is no legal authorization to access the person's criminal history. Most of the categories on the clearance card applications involve individuals applying for state certifications/licensure, such as the Arizona Department of Education teacher certification or foster care licensure through the Arizona Department of Child Safety. Eligibility to apply for a clearance card is not based solely on contact with children; it is based on qualifying for a specific category of certification/licensure or employment/volunteer designated in state statute. Currently, there is no statutory authorization for applying for a clearance card simply because a person works or volunteers with children. Applicants should be sure to check only the box or boxes which apply to them.

When the individual sends an application, including their fingerprints, to AZDPS for a clearance card, the AZDPS checks the same state and FBI databases that are checked in the fingerprint criminal history check process. This application process is between the individual and AZDPS; an agency may facilitate the application process by supplying instructions and applications, but the process does not fundamentally involve the agency. AZDPS reviews the criminal history and makes the suitability determination based on the precluding factors set out in state law; neither the individual nor the agency where the person works receive a copy of the criminal history record. The clearance card, or a denial letter if the applicant is not granted a card, is sent directly to the applicant's mailing address; for this reason and any subsequent private correspondence related to the clearance card, applicants should put their mailing address on the application, not the agency's address. An individual is denied a clearance card only if the criminal history contains one of the listed precluding offenses in either A.R.S. §§ 41-1758.03 or 41-1758.07. Subsequent Arizona arrests/convictions may result in a "file stop" and prompt a review to see if a clearance card should be suspended or revoked. The clearance card is the property of

the individual and is valid for 6 years. An agency may make a copy of it but must return it to the individual.

2.1.2 Noncriminal Justice Fingerprint Based Criminal History Check Process

The agency has legal authorization to submit applicant fingerprints to AZDPS. The process takes place between the agency and DPS; the agency submits an applicant's fingerprints and the available criminal history record is sent to the agency for review. If there is no criminal history, the AZDPS and/or FBI Results Report will indicate a negative response. The use of criminal history results is limited to the sole purpose outlined in the agency's statutory authorization to submit fingerprints. The agency must have an active user agreement on file with AZDPS and is subject to compliance regulations and periodic audits.

There is no current "file stop" program for fingerprint criminal history checks like there is for the clearance card process. The fingerprint criminal history check process is a "point in time" check, and an agency would only see changes to a person's criminal history if the fingerprints were submitted again. However, with a fingerprint criminal history check, the agency sees the actual criminal history and makes the suitability determination regarding the employee, not AZDPS. When an agency reviews the criminal history results it receives, it may find factors it wishes to consider in its employment suitability determination which would not have been considered in a Fingerprint Clearance Card determination.

2.1.3 Fingerprint Processes Chart

NCJ Fingerprint Based Criminal History Check vs. Clearance Card		
Feature	**Fingerprint Criminal History Check (Through AZDPS AIU & Applicant Teams)**	**Fingerprint Clearance Card (Through AZDPS Applicant Clearance Card Team)**
Arizona & FBI fingerprint criminal history databases checked	Yes - (unless agency authorization is for state criminal history only)	Yes
Identification card issued	No	Yes - expires in 6 years (unless suspended or revoked)
Full CHRI results reviewed by employing/licensing agency	Yes	No - AZDPS Applicant Clearance Card Team reviews CHRI
Suitability determination made by DPS	No	Yes
Suitability determination made by employing agency	Yes	No
"File stop" program for subsequent AZ CHRI	No - prints must be resubmitted to review updated results	Yes
Must have specific authorization	Yes - the authorization is specific to the agency's purpose	Yes - individual must mark the box for the proper authorization on the application
Cost	$22 regular/$20 volunteer $5 for Arizona CHRI only	$67 regular/$65 volunteer

This guide explains the submission processes and requirements for the fingerprint criminal history check process. If you have questions regarding Fingerprint Clearance Card processing, please contact the AZDPS Applicant Clearance Card Team at (602) 223-2279.

2.2 Applicant Identification

Agencies should have quality assurance processes for verifying the identity of the applicant at the time of fingerprinting to help ensure against tampering.

The Compact Council published the *Identity Verification Program Guide* containing suggestions and best practice recommendations for verifying an applicant's identity and safeguarding the integrity of the fingerprints. A copy of the guide can be downloaded from the FBI Compact Council's website at https://www.fbi.gov/services/cjis/compact-council. A link to this website can also be found on the NCJ webpage under the Overview tab (See Contact List Page 5). Compact Council recommendations regarding proper identification of applicants include:

- Accept only valid, unexpired photo identification documents as primary proof of identity, such as a state driver's license, passport, or permanent residence card.
- When accepting secondary identification (i.e., birth certificate, Social Security card), ask for supporting documentation such as a utility bill, bank statement, or mortgage documents.
- Use additional identification data support methods such as:
    - Examine the applicant's photograph on the identification provided and visually compare the picture with the applicant.
    - Compare the physical description on the documentation to the applicant's features (e.g. height, weight, hair and eye color, age, etc.)
    - Request the applicant to verbally provide a date of birth, address, etc. and verify the answers with the identification provided.
    - Check the applicant's signature provided in person with a signature on the identification provided.
    - Examine the provided identification to ensure that it has not been altered in any manner.

If the agency uses an outside agency for fingerprinting, then the agency should provide instructions to the applicant to be given to the fingerprint technician. This should include information on how to properly identify the applicant. To ensure the instructions are followed, it is recommended that the instruction form requires the fingerprint technician to record (at a minimum) the applicant's name, the type of ID presented by the applicant, and the name and company of the fingerprint technician. The form should then be returned to the agency (see the next section on "Protection of the Fingerprint Card Prior to Submission".)

2.3 Protection of the Fingerprint Card Prior to Submission

Agencies should have quality assurance processes for protecting the integrity of the fingerprint card and preventing tampering with the card from the time the prints are taken through the submission process.

Suggestions and recommendations for tampering prevention processes can be found in the National Crime Prevention and Privacy Compact Council's *Identity Verification Program Guide*. Recommendations include:

- Implement forms to standardize the information gathered with each applicant and document the type of photo identification presented by the applicant.
- Establish procedures that use sealed envelopes, agency-specific stamps, etc. for the agency to use as part of a chain-of-custody process for manually captured fingerprints.

The following process is an example:

> Agency A allows its applicants to be fingerprinted at a law enforcement agency or a nearby fingerprint service company. The applicant is provided a 9x12 brown mailing envelope containing a fingerprint card and a "Fingerprint Verification Form" which contains instructions and a section that must be completed by the fingerprint technician. The instructions inform the fingerprint technician to request a valid, unexpired government-issued photo ID and to compare the physical descriptors on the photo ID to the applicant. Once the applicant has been fingerprinted, the instructions inform the fingerprint technician to place the fingerprint card and the completed Fingerprint Verification Form into the envelope and seal it before returning the envelope to the applicant. The applicant then must deliver the envelope with the seal intact to Agency A.
>
> Additional consideration can be given to having the fingerprint technician sign their name on top of the seal, as well as having a courier from your agency pick up the fingerprint cards/envelopes from the fingerprinting site. Agencies should not accept fingerprint cards from applicants that are not in sealed envelopes or have a clear opportunity to be tampered with due to liability reasons.

There is an example "Fingerprint Verification Sheet" in Appendix A of this guide.

2.4 Identity-Verified Prints Process for IVP Clearance Cards (Schools Only)

Per Arizona Revised Statutes (ARS) §15-106, public school districts and charter schools are **required** to follow the AZDPS identity-verified fingerprints process for IVP Clearance Cards.

Identity-verified fingerprinting may be performed by a law enforcement agency, an outside fingerprinting service, or at the school district/charter school by an authorized employee. If a school district or charter school facilitates the clearance card process for employees or volunteers, the agency may want to provide instructions to the applicants to ensure that they are only fingerprinted at authorized locations and that they should have their payment ready to mail with the application and fingerprint card. The fingerprint technician should mail the IVP application, fingerprint card, and payment to AZDPS in the postage-paid envelope. To maintain the required chain-of-custody for the fingerprint card, the applicant should not be allowed to handle or take the fingerprint card with them after the fingerprints are on it.

2.5 FBI Applicant Privacy Rights Notifications

All applicants must be provided with two specific notifications that are required by the FBI, before being fingerprinted.

- The written notifications to the applicant must be provided in a format where the person can read and take a copy with him/her if desired. It is recommended, but not required,

that the written notification be presented to the applicant on a document that the applicant is required to sign.
- Simply stating that the applicant is subject to a "national background check" is NOT sufficient.

Agencies are responsible for ensuring that this information is provided at some point in their application process, whether in an in-person or online format.

Per Title 28 Code of Federal Regulations 50.12 (b), whenever an agency submits fingerprints for FBI criminal history record checks, the following actions/disclosures are required:

- The person being fingerprinted must be notified in writing that their fingerprints will be used to check the criminal history records of the FBI.
- The person being fingerprinted must be informed that they are allowed a reasonable time to complete and challenge the accuracy of the criminal history record. All applicants must be advised of this, not just those who dispute an employment/license denial.
    - If the applicant elects to review/challenge the criminal history record, the agency must provide the applicant a reasonable time to do so before final denial.
    - The agency should also establish and document what constitutes a reasonable time for the review and challenge and any appeals process that is available to the applicant. Agencies are responsible for determining what is considered a "reasonable amount of time."
- Agencies must notify applicants how to obtain a copy of the FBI record and that the guidelines for these procedures are contained in Title 28 Code of Federal Regulations 16.30 through 16.34.

The FBI also requires that all applicants be provided with the full Privacy Act Statement of 1974. Changes were made in 2019 that require applicants to be notified that while the FBI has their fingerprints in their possession (electronically), their fingerprints will cascade in their system to check for any matches to their latent print cold case files.

A copy of the *Guidelines for Required FBI Notifications of Applicant Privacy Rights and FBI Privacy Act of 1974* can be found in Appendix B of this guide and at the AZDPS website in both English and Spanish.

2.6 Basic Fingerprinting Tips

There is no certification requirement in Arizona to be able to take fingerprints. The only requirement is developing a good technique for taking clear, clean fingerprints. Agencies that are interested in doing their own fingerprinting on-site may view the "Basic Ink & Roll Training" video on our public website, provided by the AZDPS Biometrics Identification Unit.

The AZDPS does not provide fingerprinting ink. If you are going to fingerprint on-site at your agency, then you will need to obtain black fingerprinting ink. Inkless, gel, and watermark ink do not yield acceptable fingerprints.

Basic Fingerprinting Tips

Fill out the top of the fingerprint card first.

All the applicant's information should be on the card and the applicant should sign the card before taking the prints. This will avoid accidentally smudging the prints.

Have the applicant wash their hands.

Dirt or other particles on the fingers can obscure characteristics, cause smearing, and create inaccurate marks in the print. If the applicant has excessive perspiration on the hands, wipe each finger with a cloth before inking and then roll the print immediately. Using rubbing alcohol and letting it dry can also temporarily dry the skin enough to allow printing. (If using a live scan instrument, be sure that the fingerprint plate is clean and free of oils, dust, and residue from previous prints before beginning.)

Use only heavy black ink intended for fingerprinting.

Other types of ink smear or do not provide adequate coverage. "Inkless" fingerprint pads do not provide acceptable prints.

Use the right amount of ink.

Not fully inking the finger before rolling can result in "gaps" and missing characteristics in the prints. Too much ink can cause heavy smears or obscure the ridges of the print. Too little ink may result in impressions that are too faint. Fingerprints should be dark gray for the best results.

Control the person's hand.

Ask the applicant to relax and let you do the work. Asking them to look away from the card may prevent them from unconsciously "helping", which may cause twisting or slipping while trying to roll the finger.

Use the "awkward to easy" roll method.

The boxes on the fingerprint card marked for individual fingers must be rolled fingerprints. Rolled prints are made by rolling the finger or thumb from the nail edge to the nail edge. The fingerprint should show the surface of the fingerprint from fingertip to just past the first joint on the finger, and the entire print must fit within the blue lines of the box designated for that finger. Grasp the top of the applicant's hand and extend the finger to be printed. Roll in one continuous motion using only enough pressure to make a clear print with no "gaps" in the ink; too much pressure may smear the print. For best results, roll fingers on the right hand toward the right, and fingers on the left hand toward the left, going from "awkward" (where the hand/wrist is most uncomfortable) to "easy" (where the hand/wrist ends up in a comfortable natural position). This helps prevent the person from resisting and making unexpected movements as you roll. Thumbs are rolled in the opposite direction than fingers on that hand. After reaching the end of the "roll", lift the finger straight up to avoid smearing or stray ink on the card.

Position the hand well for the "flat" prints.

The bottom row of blocks on the fingerprint card is for pressed or "flat" (also known as "plain") impressions. Make sure all four fingers are extended straight and stiff from the hand. Position the hand at an approximately 45-degree angle to the card to ensure that all four fingers will fit into the box. Print as much of the fingers as you can fit, but at least to just past the first joint. Print all four fingers at the same time by pressing down; no "rolling". Press down slightly on the top of the applicant's fingers to ensure a complete print with no "gaps" and then lift straight up. Thumbs are pressed straight down into the designated block next to the finger impressions. Use care not to overlap the prints or the lines of the boxes.

Use a careful technique for "worn" fingerprints.

Some applicants may have "worn" fingerprints with thin or faint ridges. Use less ink, not more, and light pressure to achieve the best results. Squeezing the finger or "milking" it by rubbing down along the length of the finger toward the tip may help raise the ridges.

2.7 Required Information for Each Fingerprint Card

The following information is intended to assist agency personnel in ensuring that the blocks on the fingerprint card are properly completed. Either agency personnel or the applicant can fill out the card, but it is the agency's responsibility to review the information on the card for accuracy and completion and verify it with the applicant's identification. If the agency fills out the card, the applicant should review the card for accuracy before signing it. Errors, missing information, and information placed in the wrong areas can all cause delays in processing. Please type or print legibly in black ink.

2.7.1 Fingerprint Card Legend

1. **Applicant's full name**: The name should be in the last name, first name, middle name sequence.

2. **Signature**: This is the applicant’s signature. Please ensure that the applicant has signed the card in INK.

3. **Residence Address**: This is the applicant’s physical residential address, NOT the mailing address.

4. **Aliases (AKA)**: Enter any known aliases, including maiden names.

5. **ORI**: Only fingerprint cards indicating the Arizona Central State Repository (AZDPS2000) may be used. The block should be preprinted with "AZDPS2000 DPS-AFIS OPERATIONS PHOENIX, AZ".

6. **Date of birth (DOB)**: The date of birth should be in MM/DD/YYYY format.

7. **Date**: This is the date the applicant was fingerprinted.

8. **Signature of Official Taking Prints**: The signature of the person at the agency or office taking the prints should be placed in this box.

9. **Your OCA No.**: The submitting agency's ORI/OCA should be written here. This alphanumeric identifier usually starts with an "XX" and is nine characters long.

10. **Sex**: **M** for Male, **F** for Female, **U** for Unknown

11. **Race**: Enter the one-letter abbreviation for the race.

    A Asian/Pacific Islander

    B Black

    I American Indian or Alaskan Native

    W White or Hispanic

    U Unknown

12. **Height**: Enter the height in feet and inches. Example: An applicant who is 5 feet 7 inches tall should be entered as 507, not 67 inches. An applicant who is 5 feet 10 inches tall should be entered as 510.

13. **Weight**: Enter the weight in pounds as a whole number. Numbers under 100 should be entered as three numbers with a leading zero. Example: 95 pounds should be entered as 095.

14. **Eye & Hair Color:** Enter the three-letter abbreviation for the applicant's eye and hair color.

EYE COLOR	
BLK	Black
BLU	Blue
BRO	Brown
GRN	Green
GRY	Gray
HAZ	Hazel
MAR	Maroon
MUL	Multicolored
PNK	Pink

HAIR COLOR	
BLK	Black
BLN	Blond or Strawberry
BLU	Blue
BRO	Brown
GRN	Green
GRY	Gray or Partially Gray
ONG	Orange
PLE	Purple
PNK	Pink
RED	Red or Auburn
SDY	Sandy
WHI	White
XXX	Unknown or Completely Bald

15. **Place of birth**: If born in the United States, enter the two-letter state abbreviation (e.g., AZ). If the place of birth is a foreign country, enter the full name of the country (do not abbreviate).

16. **Employer and Address**: Enter the name and address of the agency that is submitting the fingerprint card. This agency must be the same agency that is assigned the ORI/OCA written in the "Your No. OCA" block.

17. **Reason fingerprinted**: Two items must be entered in this box:
    - Enter the type of position or license being applied for. Examples: "employee", "volunteer", "vendor license", "contractor".
    - Enter the approved statutory authority under which the card is being submitted. If submitting for
      FBI results in addition to Arizona records, the authorization must be currently approved by the FBI.

18. **Social Security Number**: Enter the social security number of the applicant in XXX - XX - XXXX format. If the applicant does not have a social security number, leave this blank.

19. **Miscellaneous No. MNU**: Enter the Inventory Sheet Number from the Fingerprint Card Inventory Sheet associated with the card.

20. **Rolled prints in the proper box for each finger:**
    - A complete set of inked fingerprint impressions must be submitted.

    - Fingerprints must be rolled from the side of the nail to the side of the nail. All impressions must be within the correct blue box for that print with no overlapping.

    - All impressions should be taken in proper order. The prints must be legible and classifiable.

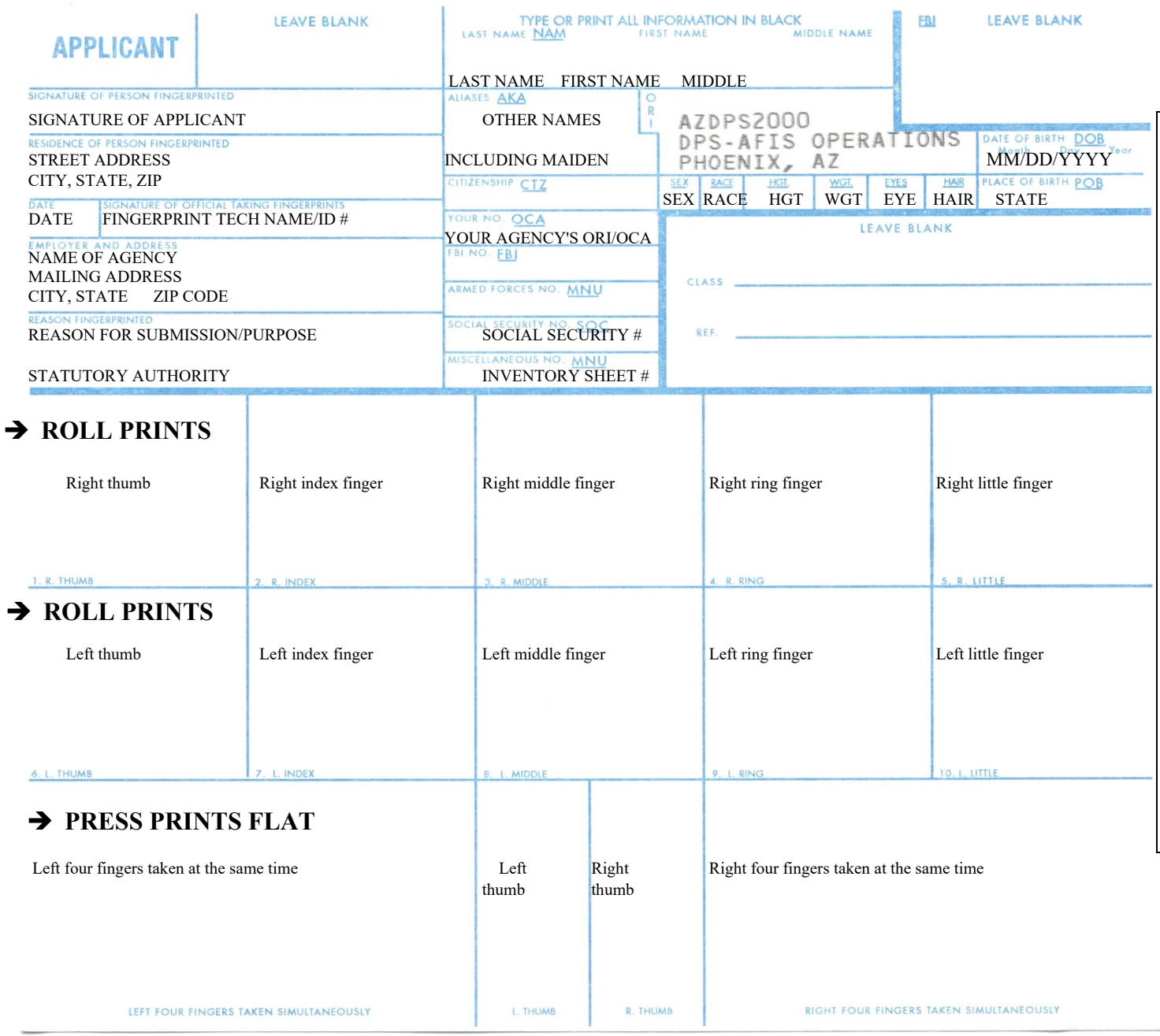
    - If a finger cannot be printed, indicate a reason in the correct finger block:
      - For a finger that was physically severed and is missing the first joint or more, you may enter "AMP" in the correct box for that finger. If the finger has been physically missing the first joint or more since birth, it is also acceptable to write "missing since birth".
      - If a portion of the first joint is still present ("tip amputated"), print the available fingerprint remainder as you normally would. If a finger is present but severely scarred, print it as you normally would.
      - Attempt to fingerprint deformed fingers; use a notation only if attempts to print have failed. If the finger cannot be printed due to injury (such as a broken bandaged finger) or severe deformation, indicate the reason for the missing print in the correct fingerprint box (e.g., "bandaged", "injured", "paralyzed").

    - See the reverse side of the card for information regarding requirements in taking a good set of fingerprints. The FBI website at www.FBI.gov offers tips for taking properly legible fingerprints. Type *Recording Legible Fingerprints* and *Capturing Legible Fingerprints* in the website search box to find these tips.

    - If a rolled print is smeared or otherwise unacceptable, you may cover it with an adhesive tab and try again. No more than two retabs may be used on a single fingerprint block.

21. **Pressed simultaneous prints in proper boxes:** Do not roll fingerprints in these boxes: these are known as "flat" or "slap" prints. Fingers are pressed down together and then lifted straight up. Thumbs are pressed down separately in the appropriate box. Ensure prints are placed in the proper boxes with no overlapping. Do not overlap the blue lines of the box.

2.8 Example Fingerprint Cards



DO NOT HIGHLIGHT ANY OF THE FINGERPRINT PORTION OF THE CARD

[1] Criminal Justice Information Services Division, United States Department of Justice Federal Bureau of Investigation. 2009. *Capturing legible fingerprints.* Correct [online image]. Retrieved 9 Aug 2012 from https://www.fbi.gov/about-us/cjis/forms/CapLegiFinger.pdf

[2] Criminal Justice Information Services Division, United States Department of Justice Federal Bureau of Investigation. 2009. *Capturing legible fingerprints.* Right four fingers have taken simultaneously correct [online image]. Retrieved 9 Aug 2012 from https://www.fbi.gov/about-us/cjis/forms/CapLegiFinger.pdf

Example Completed Card

APPLICANT

LEAVE BLANK

TYPE OR PRINT ALL INFORMATION IN BLACK

LAST NAME NAM: SMITH
FIRST NAME: JOHN
MIDDLE NAME:

FBI LEAVE BLANK

SIGNATURE OF PERSON FINGERPRINTED: John Smith

ALIASES AKA: SMITH, KEVIN
SMYTH, BILL

ORI: AZDPS2000
DPS-AFIS OPERATIONS
PHOENIX, AZ

DATE OF BIRTH DOB (Month Day Year): 10/18/1982

RESIDENCE OF PERSON FINGERPRINTED: 1 MAIN STREET
ANY TOWN, AZ 85000

CITIZENSHIP CTZ:

SEX	RACE	HGT.	WGT.	EYES	HAIR	PLACE OF BIRTH POB
M	U	602	350	BRO	BLK	AZ

DATE: 3/5/2015
SIGNATURE OF OFFICIAL TAKING FINGERPRINTS: I Am A Fingerprinter

YOUR NO. OCA: XX000000E

LEAVE BLANK

EMPLOYER AND ADDRESS: WORK INCORPORATED
1 ELM AVE
ANY TOWN, AZ 85000

FBI NO. FBI:

CLASS:

ARMED FORCES NO. MNU:

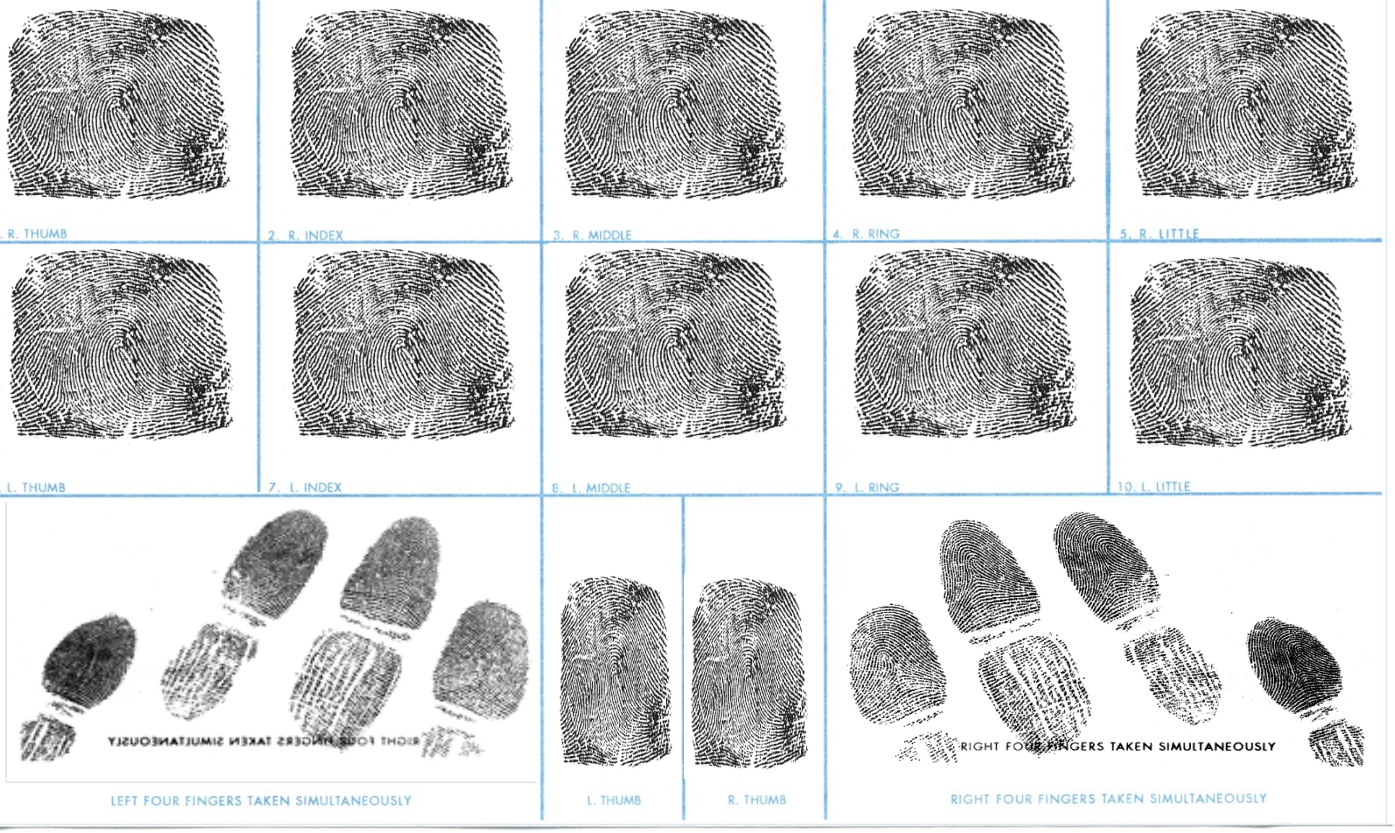
REF.:

REASON FINGERPRINTED: EMPLOYEE

SOCIAL SECURITY NO. SOC: 123-45-6789

ARS 41-1750

MISCELLANEOUS NO. MNU: 271300



2.9 Inventory Sheet

An inventory sheet must be submitted each time fingerprint cards are sent to AZDPS. The following information is intended to assist agency personnel in properly completing the blocks on the inventory sheet. Please type or print legibly and review entries to ensure that all required information has been included and matches the cards being submitted. Errors and missing information can cause delays in processing.

It is acceptable for an agency to generate its inventory sheets. An agency-generated inventory sheet must contain all information in Section 2.9.1, including a non-repeating, six-digit Inventory Sheet Number.

2.9.1 Inventory Sheet Legend

1. **Date:** Enter the date the sheet is being submitted.

2. **Submitting Agency's Name:** Enter the submitting agency name.

3. **Submitting Agency's ORI/OCA Number:** Enter the submitting agency ORI/OCA number. This is the nine-digit alphanumeric identifier beginning with "XX" – the same identifier entered in the "Your No. OCA" block on the fingerprint card.

4. **Type of Applicant (s):** Mark the type of applicants listed on the sheet. Mark ONLY one box – different types of applicants must be listed on different inventory sheets. (Example: Use one inventory sheet for regular applicants but use a second inventory sheet for volunteers.) If your agency submits fingerprints for Arizona results ONLY (no FBI check), then mark the "state-level only" box regardless of the type of applicant.

5. **Direct Phone of Contact Person:** Enter the telephone number of the person DPS should contact if there are questions about the submission packet.

6. **Applicant's Name:** List applicants in alphabetical order according to the last name. A maximum of 30 applicants can be listed on one inventory sheet. Use a separate inventory sheet for additional applicants or different types of applicants. To reduce processing time, submit as many of the same types of applicants on as few inventory sheets as possible.

7. **Date of Birth:** Enter the subject's date of birth in MM/DD/YY format.

2.9.2 Inventory Sheet Distribution

A sample inventory sheet is included on the next page. An actual inventory sheet has two copies.

- Copy 1 (white copy) should be submitted along with the full payment and the associated fingerprint card(s).

- Copy 2 (canary copy) is for the submitting agency's files. Your agency is required to save the current and the previous years' inventory sheets. Any other inventory sheets may be discarded. The auditor will only request the previous years' inventory sheets.

ARIZONA DEPARTMENT OF PUBLIC SAFETY

NON-CRIMINAL JUSTICE APPLICANT FINGERPRINT CARD INVENTORY SHEET

Inventory Sheet Number
271300

Applicant Team ☎ **(602) 223-2223**

Date	Submitting Agency	Submitting Agency's ORI/OCA Number
8/10/2016	Work Incorporated	XX000000E

Type of Applicant(s) (Check One Box Only)

- ☒ **Regular Applicants**
- ☐ **Volunteers**
- ☐ **Resubmits** (No Fee Required)
- ☐ **State Level Only**

Direct Phone Number of Contact Person
602-000-0000

	Applicant's Name	Date of Birth
1	Smith, John	10/18/1982
2	Vaughan, Tom	09/23/1937
3	White, Madge	01/01/1962
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
29		
30		

SAMPLE ONLY

✓ Applicant Fingerprint Card Submission Checklist

- ☐ ↖ **Check the box that corresponds to the type of applicant(s) being submitted with this sheet.** Submit separate sheets for each type of applicant (for example, volunteers and regular applicants cannot be submitted on the same sheet).
- ☐ ← **Write applicants name and date of birth legibly with the last name first.** Do not submit more than 30 names per sheet; if more than one applicant, complete the list in alphabetical order using the last name.
- ☐ ← **Enclose payment in the *exact* amount required.** No more than three forms of payment can be accepted per sheet; forms of payment accepted are Money Orders, Cashier's Checks and business checks. We do not accept personal checks or cash. You may provide one form of payment for up to 35 inventory sheets as long as only one type of applicant is being submitted.
- ☐ ↓ **Mail this sheet, the corresponding applicant fingerprint card(s) and payment to the address shown below.** Do not include additional paperwork with your submission unless otherwise instructed.
- ☐ Keep the canary copy for your files.
- ☐ Do not staple items to this sheet. Use a paperclip.
- ☐ Do not make copies of this inventory sheet for reuse; this sheet number is unique and cannot be duplicated.
- ☐ Do not use this inventory sheet for criminal justice applicants.

Applicant Team
Mail Drop 3190
P.O. Box 18430
Phoenix, AZ 85005-8430

DPS 802-06513 Rev. 02-2017

2.10 Payment and Submission Packets

This subsection contains fee information and payment submittal requirements.

2.10.1 Fees

(Current fees as of October 2020)

Regular Applicant (state and FBI checks)	$22.00 per card
Applicants who are volunteers working with minors, the elderly, or the disabled	$20.00 per card
State-Level only (only checks Arizona records)	$5.00 per card

2.10.2 Payment Submittal Requirements

All noncriminal justice applicant fingerprint cards should be accompanied by a cashier's check, money order, or agency check to cover the total processing costs of the submitted fingerprint cards. (Agencies using the Arizona Financial Information System (AFIS) may send transfers through AFIS. Be sure to attach the *State Agency Submission Sheet*, located in Appendix C of this guide, along with the fingerprint submission packet.)

AZDPS does not accept personal checks, cash, or credit/debit cards.

Payment guidelines:

- Make the payment instrument payable to the **Arizona Department of Public Safety**.
- If a receipt is desired, submit a completed receipt form and a self-addressed stamped envelope.
- A maximum of three forms of payment may be submitted with any single inventory sheet.
  - Example: If there are five money orders at $22.00, attach the first three money orders to one inventory sheet with the associated fingerprint cards. Then attach the other two money orders to another inventory sheet with the associated fingerprint cards.
- No more than 30 inventory sheets may be submitted in conjunction with any single payment instrument. If there are more than 30 inventory sheets full of names, please submit a separate check for those inventory sheet(s) over 30 along with the associated fingerprint cards.
- The AZDPS Applicant Team cannot accept personal checks from applicants; direct deposit of applicants' personal checks to the AZDPS account through the state treasurer's office is not allowed. Personal checks should be deposited in the submitting agency's account and funds subsequently transferred to AZDPS using a company check.
- If a discrepancy is found in either the amount or method of payment, the entire submission packet will be returned.

2.10.3 Submission Packet

Submissions MUST include all the following:

- ☑ Inventory sheet (DPS form # 802-06513)
- ☑ Fingerprint cards for applicants listed on the inventory sheet
- ☑ Correct payment in the exact amount for all included cards

Send completed fingerprint packets to

Arizona Department of Public Safety
Applicant Team
P.O. Box 18430 | MD 3190
Phoenix AZ 85005-8430

2.11 Rejected Fingerprint Cards/Resubmissions

When fingerprint submissions are rejected, you will receive an AZDPS and/or an FBI notice with the reason for the rejection.

Generally, if a card is rejected for payment reasons, you can correct the payment discrepancy and resubmit the cards. No new inventory sheet is needed. Be sure to follow the instructions in the notice accompanying the rejected card(s). Section 2.10 of this guide has more information on payment requirements.

If cards are rejected for incomplete/inaccurate information, carefully follow the instructions on the reject notice. Depending on the reason for the reject, you may need to submit a new inventory sheet or resubmit the entire packet. If you must use a new inventory sheet, remember to change the inventory sheet number on the fingerprint card. You can cross out the previous one and write in the new one if there is room, or you may cover the old number using an appropriately sized tab or "white-out" tape. Always submit a copy of the reject notice when you resubmit cards.

If the fingerprint cards were rejected because the fingerprints are illegible or unclassifiable, a new fingerprint card will be needed. You will need to complete a new inventory sheet and mark the "resubmit" box. Always include a copy of the reject notice/FBI reject sheet with your resubmission

Example AZDPS (Front-End) Reject Slip

ARIZONA DEPARTMENT OF PUBLIC SAFETY

APPLICANT FINGERPRINT CARD RETURN NOTICE

- ☐ Fingerprint(s) does NOT include crease of first joint to tip of finger.
- ☐ For livescan use a printer with 1200 DPI
- ☐ Only two retabs allowed per block
- ☐ Before reprinting
  - ☐ condition hands with lotion for several days
  - ☐ avoid chemicals
  - ☐ wear gloves when possible
- ☐ Out of sequence
- ☐ Moist fingers (wipe with rubbing alcohol)
- ☐ Dry fingers, use lotion / water
- ☐ Do not use a stamp pad
- ☐ Prints smudged
- ☐ Poor ridge quality
- ☐ Prints too light / dark
- ☐ Quality of images too low to be used

Reasons for reject

RECOMMENDATIONS:	
AFPS BADGE NO.	TODAY'S DATE

DPS 802-07079 Rev. 2-2020

Example FBI Reject Sheet

REJECT

1.01: 158
1.02: 0201
1.03: 1
1.04: ERRT
1.05: 20021124
1.06: 4
1.07: WVIAFIS0Z
1.08: WVIAFIS0Z
1.09: IFCS000X151902662170
1.10: 2A09000030
1.11: 00.00
1.12: 00.00

2.001: 466
2.002: 00
2.006: XX000000E
2.060: L0008 – THE QUALITY OF THE CHARACTERISTICS IS TOO LOW TO BE USED. HOWEVER, POSSIBLE CANDIDATES WERE FOUND. PLEASE SUBMIT A NEW SET OF FINGERPRINTS FOR COMPARISON TO THE CANDIDATE(S).
2.073: AZDPS2000

Reason for reject

Applicant cards rejected by AZDPS or the FBI for poor print quality can be resubmitted one time, free of charge; however, the resubmitted card must be received within one calendar year of the date of the original rejection.

2.11.1 Routine Name Search Procedure

A routine name search requests a name, date of birth, and Social Security number check on an applicant whose fingerprints have been rejected twice by AZDPS or the FBI.

The agency must follow the routine name search procedure if the fingerprints are rejected a second time because the fingerprints are illegible or unclassifiable or if the agency is required to present a page with the applicant's name on it to prove negative name search results.

Routine Name Search Procedure

1) The fingerprints must have been rejected twice by AZDPS and/or the FBI.
   a) The first reject must be within the past year.
   b) The name search request must be submitted within 90 days following the second reject.
   c) If the above time parameters are not met, the applicant must start the fingerprinting submission process again, including the fee.

2) The agency must complete and submit the CJIS Name Search Request Form located in Appendix D of this guide. The PCN is the number below the bar code on the fingerprint card. Enter the PCN of the last two fingerprint cards that were rejected. Write your agency's ORI/OCA in the OCA field. When the form is completed, FAX the form to the Applicant Team along with the applicant's two DPS or FBI reject notices. It takes two to three days to receive the results back from the FBI depending on their volume. The results will be forwarded to your agency.

If the request cannot be processed, it will be faxed back with a reject notice indicating why they could not complete the request.

2.12 State Fingerprint Results

The state results sent by AZDPS will consist of the submitted fingerprint card and any Arizona warrants, Arizona sex offender registrations, and Arizona criminal history information. These results will also include a Results Report summary sheet; this page lists all the applicants that were contained on the inventory sheet sent by the agency and indicate results in the State FP Result and NCIC/ACIC Result columns.

PLEASE SEND A REQUEST FOR A COPY OF THE FULL NCJ AGENCY GUIDE FOR EXAMPLES OF CRIMINAL JUSTICE INFORMATION (CJI) AND CRIMINAL HISTORY RECORDS INFORMATION (CHRI) TO NCJA@AZDPS.GOV

2.13 FBI Results

The FBI criminal history results will be on the same Results Page as the state-level results. The results report page will contain all the applicants that were listed on a single inventory sheet.

PLEASE SEND A REQUEST FOR A COPY OF THE FULL NCJ AGENCY GUIDE FOR EXAMPLES OF CRIMINAL JUSTICE INFORMATION (CJI) AND CRIMINAL HISTORY RECORDS INFORMATION (CHRI) TO NCJA@AZDPS.GOV

Section 3 - Basic Privacy & Security Guidelines

Access, use, handling, dissemination, and destruction of criminal justice information (CJI) and criminal history record information (CHRI) is governed by federal and state laws, rules, regulations, and policies. The receiving organization is responsible for maintaining the confidentiality and control of any CJI/CHRI it obtains. CJI/CHRI may ONLY be used for the specific purpose for which it was requested (employment, licensing, volunteers, etc.).

3.1 Policies and Procedures

The agency must establish policies/procedures in the following CJI/CHRI privacy and security areas, and ensure all organization personnel are aware of them. Agencies may utilize the "Noncriminal Justice Compliance Worksheet" to help guide them through the process of creating agency-specific policies and procedures, or the "Example Noncriminal Justice Compliance Policy & Procedure" Template. If an agency chooses to use the Template, the agency name will need to be inserted as well as some agency-specific choices regarding this program participation.

- Access:
  - Defining who is authorized to access CJI/CHRI
  - Restricting access to only those who are authorized
- Use:
  - Defining the authority, purpose, and use of the CJI/CHRI
  - Restricting use to the specific purpose for which the CJI/CHRI was requested
- Handling:
  - Proper security of CJI/CHRI from receipt through destruction
  - Retention/destruction rules and processes
- Prevention of unauthorized disclosure of CJI/CHRI:
  - Access-limited storage
  - Not leaving CJI/CHRI unattended when it is not physically secured
  - Revocation of access privileges for terminated employees or those removed from the Authorized Personnel List
  - Processes for ensuring proper training and refresher training of Authorized Personnel
- Communication:
  - Communication among Authorized Personnel
  - Communication with the applicant concerning CJI/CHRI
- Secondary dissemination procedures (if permitted by law):
  - Logging/tracking procedures
  - Procedures for authenticating recipients of the disseminated information
- Formal disciplinary procedure:
  - Steps to be taken by the organization in the event of misuse of CJI/CHRI
  - Specify applicable misconduct policies
- Digital security (if CJI/CHRI scanned or stored electronically):
  - Technical safeguards to protect the access and integrity of confidential information
  - Monitoring and restricting access to databases containing CJI/CHRI
  - Reporting, response, and handling capability for information security incidents

Additionally, agencies should have established processes for fingerprint submissions which include:

- Quality assurance measures for applicant identity verification. (See Section 2.2)
- Quality assurance measures for protecting the integrity of the fingerprint card. (See Section 2.3)
- Processes to ensure compliance with federal laws for FBI fingerprint checks (if applicable). (See Section 2.5)

The agency should consider the following basic guidelines when formulating policies, procedures, and training.

3.2 Applicant Process

The employing/licensing agency may verbally discuss the criminal record contents with the applicant within the confines of the purpose for which it was provided:

- The agency may inform the applicant that the application is denied due to precluding factors found during the criminal history check and identify the factors.
- The agency may tell the applicant that there is a factor in the criminal history check that may be disqualifying and discuss that factor with the applicant to ascertain if the circumstances of the issue warrant denial.
- The agency MAY NOT provide a copy of the criminal history record to the applicant. To obtain a copy for review or to challenge the contents of a criminal history record, the applicant needs to follow procedures delineated by law for review and challenge. (See Section 3.3)
- Agencies must take care not to include any of this information in employment/license rejection letters.
- CHRI should not be discussed in public meetings or forums, however, public court or police records MAY be used and discussed.
- CHRI can only be shared with Review Boards if all in attendance are on the Authorized Personnel List. Sharing CHRI with third-party legal representation is not permitted.

3.3 Applicant Review and Challenge of Criminal History

It is the agency's responsibility to notify applicants of the opportunity and ability to review and challenge a criminal history record. If an applicant feels his/her criminal history record is inaccurate or incomplete, refer the person to the appropriate contact below to begin the review and challenge process. **DO NOT** provide the individual a copy of the record.

- For a copy of an Arizona criminal history record:
  - The individual can contact the Department of Public Safety Criminal History Records Unit at
    (602) 223-2222 to obtain a fingerprint card and a Review and Challenge packet, or the individual can download information from the Criminal History Records Unit section of the DPS website. The Department of Public Safety provides the review and challenge packet pursuant to R13-1-08 of the Arizona Administrative Code.
  - This will check the Arizona criminal history only.

- For a copy of an FBI criminal history record:
  - U.S. Department of Justice Order rules and federal law allow the subject of an FBI record to request a copy of his/her record. The individual may submit fingerprints, an Applicant Information Form, and payment directly to the FBI according to the procedures in Title 28 Code of Federal Regulations §16.30 - 16.34.

- FBI contact phone for information about record review and challenge: (304) 625-5590.
- Submittal forms, checklists, and more information on how to review and challenge an FBI criminal history record can be found at http://www.fbi.gov under *Criminal Justice Information Services - Identity History Summary Checks*.

3.4 Communication/Dissemination

Verbal or written communications regarding CJI/CHRI may only occur between personnel authorized to possess the information and only to carry out the specific purpose for which the information was requested.

3.4.1 Communication Cautions

Agency personnel should be aware of the following restrictions and cautions concerning CJI/CHRI:

- CJI/CHRI received from the fingerprint criminal history check process is not public record and may not be released to the public. The agency may neither confirm nor deny the existence or nonexistence of an individual's criminal history record to the public or any unauthorized individual or agency.
- Care should be taken to prevent overhearing, eavesdropping, or interception of communication. Consider using private rooms, closed offices, etc., when discussing CJI/CHRI with other authorized personnel or with applicants.

- Viewing and/or disseminating CJI/CHRI for curiosity reasons is not allowed.

- CJI/CHRI cannot be:
  - Emailed (unless encrypted)
  - Sent electronically via cell phone or other handheld devices (including texts or pictures of the hardcopy or computer screen)

- CJI/CHRI may be faxed only if:
  - The recipient point is within the agency or secondary dissemination is authorized.
  - The recipient has been confirmed by the sender as Authorized Personnel or as an otherwise authorized recipient.
  - The receiving fax is in a secure location controlled by the authorized recipient and the arriving CJI/CHRI is not accessible to unauthorized personnel. The agency is responsible for the security of all copies of CJI/CHRI.

- Personnel should be cautioned regarding common causes of casual unauthorized release of information: (e.g., social networks, discussions with friends/family members, conversations in public places.)

- Personnel should be made aware of the threat of social engineering. Social engineering is deliberate manipulation or deception designed to elicit the release of confidential information to unauthorized individuals. If secondary dissemination is permitted, the agency should develop a method that allows personnel to verify the identity and authorized status of an individual requesting information both inside and outside the agency.

3.4.2 Secondary Dissemination

The receiving agency may not provide CJI/CHRI to any other agency or individual unless specifically authorized by law. This is called "secondary dissemination". For example, school district A may not share CJI/CHRI with school district B, even though the purpose is the same. Two individual non-profit agencies that fall under the same board are not permitted to share CJI/CHRI as they are considered separate entities.

Secondary dissemination can only occur with an authorized recipient. All secondary dissemination must be logged, and the log shall be retained for three years. The log should identify the following:

a) Date of dissemination
b) Name of requestor
c) Name and contact information of requestor's agency
d) Purpose for which information is requested
e) Specific information being released (i.e., criminal history of name of subject)
f) The name/identification of the person releasing the information

3.5 Physical Security

The user agency is responsible for the security of the CJI/CHRI from its arrival at the agency through the point of its destruction.

3.5.1 Storage

The results of the state and/or FBI record search should be stored in such a manner that only authorized agency personnel to have access and should not be retained longer than needed to fulfill its purpose and satisfy the agency's regulatory guidelines.

- CJI/CHRI must be maintained at all times in a secure location to prevent access/viewing by unauthorized personnel (i.e., locked file cabinet, locked room, secure perimeter, etc.).

- All visitors (including contractors, maintenance, and outside personnel) to areas where CJI/CHRI is kept must be accompanied by authorized staff personnel at all times. Areas must be locked when unattended.

- Personnel who are granted access to CJI/CHRI must be aware of their responsibility to protect the confidentiality of the information and take steps accordingly. Examples of this are: turning pages with CJI/CHRI face down on a desk; not leaving information exposed or unattended; turning or covering computer screens to inhibit casual viewing; being aware of unauthorized individuals who may be "shoulder surfing" or walking by when information is being viewed.

- If the organization is a public agency that stores records at the Arizona State Library, Archives and Public Record Department, all CJI/CHRI must be removed before releasing the record for storage and/or eventual destruction. It is recommended that CJI/CHRI be maintained separately from any files which may be considered public record.

3.5.2 Destruction

When no longer needed for its purpose, CJI/CHRI must be destroyed to minimize the risk of unauthorized access and dissemination.

- CJI/CHRI cannot simply be thrown away. The acceptable methods of destruction are shredding or incineration. Destruction must be performed or observed by personnel who are authorized to access/handle CJI/CHRI.

- Electronic media holding CJI/CHRI must first be sanitized (overwritten at least three times, degaussed) before destruction.

3.6 Technical/Digital Security

If the CJI/CHRI sheets are stored electronically, or CJI/CHRI derived from the sheets is stored electronically, then the agency becomes subject to technical information security requirements.

The requirements for electronic storage and access of CJI/CHRI are contained in the FBI CJIS Security Policy which can be viewed in the online FBI CJIS Security Policy Resource Center on the FBI website at *www.fbi.gov*. Electronic security, encryption, and storage protection requirements in the policy apply to agencies converting hardcopy CJI/CHRI into electronic format after receipt; the parts governing direct connect/interface with the state/national electronic criminal justice databases do not apply unless the agency has an additional function with direct connect/interface access. Agencies should have knowledgeable information technology (IT) personnel review the requirements in the Security Policy and ensure that agency's system is in compliance.

The following general guidelines also apply to electronic/digital security of CJI/CHRI:

1) The server must be secure and located either on-site with that agency or on a site controlled by the agency.
    - The actual location of the computers and servers must have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment or any of the stored data.
    - Only employees of the agency, including IT personnel, may have access to the server.

2) Authorized Personnel who access CJI/CHRI electronically must complete additional portions of the CJIS Online training which pertain to electronic access.

3) The agency must manage information system accounts. Requirements include:
    - Processes for activating, reviewing, and disabling accounts.
        - The files where CJI/CHRI is stored must be password-protected.
        - Each individual accessing the CJI/CHRI files must be uniquely identified and have a unique password.
        - Password rules are detailed in the Security Policy.
    - Processes for authorizing and monitoring remote access (if applicable).
    - Restrictions regarding the use of personally owned electronic devices to access, handle, or store CJI/CHRI.
    - Electronic media protection rules, to include provisions for destruction which include degaussing, overwriting, or physical destruction of media.

4) The computer system must have protective features that are detailed in the Security Policy. These include but are not limited to:
    - Partitioning which physically or logically separates user interface services from information storage databases
    - Intrusion detection/Malicious code protection

- Spam and spyware detection/protection

5) An incident response procedure must be in place which allows users to alert technical personnel to an information security incident such as an unauthorized system intrusion. The incident handling response must include preparation, detection and analysis, containment, eradication, and recovery.

3.7 Consequences for Misuse

The receiving agency has the responsibility to ensure that all personnel is aware of the consequences that may result from the unauthorized use of CJI/CHRI. The AIU must be promptly notified of any cases of misuse within an agency.

Arizona Revised Statute §41-1756 states it is a class 6 felony in Arizona for a person to:

- Provide criminal history record information to someone who is not authorized to receive it.
- Allow unauthorized access to criminal history information.
- Use criminal history record information for any other purpose other than those provided for in ARS§ 41-1750.

Federal statutes state that access to CJI/CHRI is subject to cancellation for dissemination outside the authorized recipient(s) (Title 28 USC §534 and Title 28 CFR §20.33). An agency's access to CJI/CHRI via submitted fingerprints may also be suspended or canceled according to the Terms and Conditions in the user agreement.

Other federal and/or state penalties may apply depending on the circumstances of the release and the specific statute which is violated. Two examples of United States Code violations are Title 18 USC § 641 which deals with the theft of public records for personal gain and Title 18 USC § 1030 which discusses unauthorized access to protected information via computer.

An unauthorized release could potentially expose the organization and/or individual to civil liability. Also, an individual may be subject to disciplinary action under his/her employer's misconduct policies.

Section 4 - ASC Responsibilities

As mentioned in Section 1 of this guide, the user agreement requires each agency to designate an Agency Security Contact (ASC). The ASC is the primary liaison between the user agency and AZDPS and is responsible for coordinating agency compliance with all federal and state laws/regulations about the access, use, handling, dissemination, and destruction of criminal justice information and criminal history record information. This section summarizes the primary duties and responsibilities of the ASC.

4.1 Primary Liaison

The ASC functions as the primary liaison with AZDPS for all communication regarding audits, training, and security. The ASC is also the first point of contact for AZDPS in the event of an allegation of criminal history misuse or a security issue involving the criminal history check process. The ASC's contact information must stay updated with the AZDPS Access Integrity Unit to allow for an orderly and timely exchange of information.

The ASC is also expected to serve as the information resource for his/her agency. The Noncriminal Justice Compliance Team sends periodic emails to the ASC to keep agencies updated on changes and events relevant to the noncriminal justice process. The ASC is expected to share this information with the personnel at the user agency as needed.

The Applicant Team (the team which processes the fingerprint submissions and sends out the CJI/CHRI results) also usually maintains a contact person at each agency in case of a processing problem. Agencies may choose to have the ASC serve in both capacities or may choose to have a different person for each, based on the agency's organizational structure and need. Both contacts should be kept updated.

4.1.1 Information Changes

In addition to keeping the ASC's contact information updated, the ASC is responsible for keeping the agency's information updated. The ASC should inform the AIU Noncriminal Justice Compliance Team of changes in the CEO, the ASC, or any relevant business information (agency name changes, mailing/physical address changes, etc.). The forms mentioned in this section are in the appendices of this guide and are also available from the DPS website at www.azdps.gov/services/government/ncj. Forms may be emailed, faxed, or mailed to the Access Integrity Unit. (See the **Contact List** on page 4.)

- If the signatory to the User Agreement changes:
    - The agency must sign a new user agreement within 30 days or access will be suspended.
- If the ASC changes:
    - The agency must appoint a new ASC and submit the *Noncriminal Justice Agency Information Change Form* to the AIU Noncriminal Justice Compliance Team within 30 days of the change. (See Appendix E for a copy of this form or the DPS website.)
    - For the agency's convenience, this form allows the agency to change the Applicant Team contact as well. If this box on the form is checked, then the Noncriminal Justice Compliance Team will update the contact with the Applicant Team.
    - The agency can also designate a secondary (backup) ASC on this form. The Noncriminal Justice Compliance Team will send an email acknowledgment upon receipt of the notification.

- If the CEO changes:
    - Submit the *Noncriminal Justice Agency Information Change Form* to the AIU Noncriminal Justice Compliance Team. (See Appendix E or the AZDPS website.) If the new CEO has not been selected, submit the information of the interim/acting CEO and note the anticipated time before permanent replacement in the form's Comments field.
    - AZDPS will provide a new User Agreement with instructions for its completion if needed.
- If the name, mailing address, physical address, and/or main phone number of the agency changes:
    - Fill out the information you want to change on the *Noncriminal Justice Agency Information Change Form*. (See Appendix E or the AZDPS website.)
    - The Noncriminal Justice Compliance Team will acknowledge receipt of the form and update the information with the AZDPS Applicant Team, if applicable. If further information is required, a Noncriminal Justice Compliance Specialist will contact the ASC with any questions.
- If the legal authorization changes:
    - The ASC must submit the new authorization to the Noncriminal Justice Compliance Team who will forward this information to the FBI Criminal Justice Information Law Unit for review.

4.1.2 Authorized Personnel List

The ASC must submit an APL to the AIU Noncriminal Justice Compliance Team. The APL contains all agency personnel who are authorized to receive, view, handle, disseminate, store, retrieve, or dispose of CJI/CHRI. The APL should be submitted on the agency's letterhead and should contain the names and titles of the authorized individuals.

Examples of types of personnel an agency may want to authorize:

- Administrative personnel who open the agency's mail, have filing duties or perform functions which grant them trusted access to locked/secured areas or access to unsealed CJI/CHRI.
- Personnel involved in employment/position suitability determinations: human resources personnel, directors, supervisors, appeals board members, interviewers, etc.
- Information technology personnel (if CJI/CHRI is stored electronically).

An example APL can be found in Appendix F of this guide and online on the AZDPS website. The entire APL must be updated and resubmitted when changes occur (e.g., an individual is no longer authorized to view/handle CJI/CHRI, an authorized individual is no longer employed by the agency, an authorized individual has a name change, personnel turnover, and name/contact information changes). Ensure the ASC is on the Authorized Personnel List. The agency should retain one copy of the APL for its records and forward a copy to the AIU Noncriminal Justice Compliance Team.

The FBI requires that all personnel with unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas where CJI/CHRI is housed receive a state of residency and national fingerprint-based background investigation before receiving access. Agencies should use A.R.S. § 41-1750 as the statutory authority for doing so.

4.2 Privacy and Security Coordinator

The ASC is the person primarily responsible for maintaining agency compliance with state and federal rules for privacy and security requirements. Compliance duties include:

- Ensuring Authorized Personnel receive required training.
- Updating/maintaining training documentation.
- Ensuring Authorized Personnel have signed the agency's Acknowledgement Statement.
- Ensuring the agency has adequate policies/procedures related to access, use, handling, dissemination, and destruction of CJI/CHRI.

4.2.1 Required Training for Authorized Personnel

Authorized Personnel must complete two sets of training:

1) CJIS Online Training:
   CJIS Online is the minimum basic Security Awareness training required for all individuals (criminal justice and noncriminal justice) who view or handle criminal history information. All Authorized Personnel must receive CJIS Online training (Level 4) within six months of hire or be placed on the Authorized Personnel List and then every two years thereafter. The training is located on the internet at www.CJISOnline.com. The CJIS Online Training Supplement for Noncriminal Justice Agencies contains the log-in information for CJIS Online and is designed to explain and clarify points in the online training for those individuals who have no background in the criminal justice field. The supplement is available for download at the AZDPS website.

2) Agency's policies/procedures training:
   Each agency must train Authorized Personnel on the agency's internal policies/procedures for the proper access, use, handling, dissemination, and destruction of CJI/CHRI and the consequences of misuse of CJI/CHRI; training must be conducted within six months of hire or being placed on the APL and then every two years thereafter. The agency is required, under the user agreement, to have the internal handling procedures; more information on the required policies/procedures is available in Section **3.1** and Section **5.2**. The ASC must ensure that the training curriculum is adequate and covers the required topics. Training outlines will be reviewed by the AIU Noncriminal Justice Compliance Team during audits.

The ASC is responsible for maintaining and updating the Training Documentation Form showing that both CJIS Online and agency internal privacy and security training have been completed. **Authorized Personnel DO NOT need to come to AZDPS for training**. AZDPS's compliance training is designed to help the ASC or other designated agency representatives understand the new compliance requirements so that they can implement the rules back at their agency; AZDPS training does not take the place of the user agency's internal training. Training Documentation Forms need to be kept on file at the user agency and must be forwarded to the AIU Noncriminal Justice Compliance Team upon request. A blank Training Documentation Form is located in Appendix G of this guide and is also available for download at the AZDPS website.

4.2.2 Acknowledgement Statements

All authorized personnel must sign a statement acknowledging notification of the penalties for misuse of the information. There is no standard format for the Acknowledgement Statement. It must state at a minimum that the undersigned "acknowledges notification for the penalties for misuse of criminal justice and criminal history record information" but ideally it contains a summary of state, federal, and agency consequences. Some agencies choose to add a short training outline to the statement so that the employee specifically acknowledges their training as

well. Acknowledgment statements only need to be signed once, although an agency may choose to do so more frequently.

The ASC is responsible for entering the date Acknowledgement Statements were signed on the Training Documentation form. Do not send the acknowledgment statements to AZDPS; keep the forms on file at the agency. AIU Noncriminal Justice Compliance personnel will review these forms during the agency's audit.

4.3 Audit Responsibilities

The ASC is the agency's representative for all audits and cooperates with state and federal officials throughout the audit process. More details on the audit process are contained in **Section 5.**

The ASC's responsibilities during an audit include:

- Ensuring all the audit instructions are followed and that the packet is returned promptly.
- Being present for the audit interview and notifying/gathering any other agency personnel who might be needed to answer the auditor's questions.
- Having all requested documentation available for the audit.
- Serving as the primary coordinator for any corrective actions stemming from the audit findings.

Section 5 - Audits & Compliance

Agencies that are enrolled in the Noncriminal Justice Fingerprint Compliance Program are subject to an audit to ensure compliance with state and federal rules regarding fingerprint submissions and CJI/CHRI use. This section explains the general audit process and discusses the Arizona Noncriminal Justice Compliance Program requirements.

5.1 Audits

In Arizona, a routine audit cycle has been established for noncriminal justice agencies to assess compliance with state and federal policies and regulations. AZDPS AIU personnel conduct the audits.

5.1.1 Routine Audits

A routine audit is a scheduled review of the agency's compliance with the Noncriminal Justice Compliance Program requirements. The AIU Noncriminal Justice Compliance Team will notify the agency approximately 30 days in advance of the planned audit date. The notification will describe the audit process and provide the contact information of the assigned auditor (Compliance Specialist). The ASC should contact the Compliance Specialist to acknowledge receipt of the audit notification.

The notification will state whether the agency is scheduled for a telephonic or an in-person audit. The ASC must be present for the audit; the agency may also have other personnel in attendance if needed or desired. Compliance assessment documents will be sent with the notification; these documents will need to be completed and returned by the date indicated on the accompanying audit timeline.

The Compliance Specialist will conduct a complete file review of the agency before the audit interview. All documentation relating to general administration, fingerprint submissions, privacy and security, and training will be reviewed at or before the audit interview. The ASC will be asked to complete an assessment questionnaire and a chart as part of the pre-interview process.

After an audit has been completed, the Compliance Specialist will provide the agency with a written report which will either denote complete compliance or will contain recommendations for corrective actions to bring the agency into compliance. Compliance Specialists are available to discuss specific concerns and to offer training to assist the agency in this process.

5.1.2 Directed Audits

A directed audit is an administrative review prompted as a result of an incident or allegation of possible misuse of CJI/CHRI. Most issues of misuse stem from instances of improper dissemination of criminal history record information to unauthorized individuals or agencies.

AIU may conduct a directed audit of an agency if AZDPS:

- Receives a complaint from an agency or individual alleging misuse of CJI/CHRI.
- Becomes aware of agency actions that may constitute a misuse of CJI/CHRI.
- Becomes aware of agency actions which may be a violation of the user agreement terms.

A Compliance Specialist from the AIU will contact the agency's ASC and arrange to conduct a review of the agency's processes and actions which may have resulted in a misuse. If the agency

cannot reach the ASC within a reasonable time, AZDPS will contact the ASC's supervisor, agency CEO, or another representative.

The review by an AIU Compliance Specialist is designed to detect process issues that may result in non-compliant actions by an agency. Areas that will be audited are the same ones that are checked during a routine audit; also, the review may focus on the policies, procedures, process, and actions most closely related to the allegation. Compliance Specialists will ask questions regarding the circumstances surrounding the allegation to determine if/how the incident occurred and what actions might be required to prevent a repeat of any misuse. The ASC should be present for the audit as well as any other personnel the agency deems necessary. Following the directed audit, the Compliance Specialist will prepare a written report of his/her findings. If compliance issues are detected, the report will contain recommendations and/or specific requests to bring the agency into compliance so that it can continue to utilize the fingerprint criminal history check process through AZDPS. The agency will be required to respond in writing regarding its corrective actions in the areas of concern.

A directed audit does not replace a routine audit. If a directed audit finds issues that require correction, an agency may be scheduled for a routine audit after a specified period to reassess agency compliance.

5.2 Compliance Review

This subsection discusses the general compliance requirements for each of the areas reviewed by Compliance Specialist auditors: general administration, fingerprint submissions, privacy and security, and training. Each part contains a short explanation of the requirements and may reference different resources or areas of the guide which an agency may refer to for more information.

5.2.1 General Administration

The general administration section of an audit reviews the basic information on file for the agency for completeness, accuracy, and compliance with current regulations.

1) User Agreement (Section **1.2**)
   The user agreement is the contractual agreement between the user agency and AZDPS that allows AZDPS to provide CJI/CHRI upon the submission of fingerprints. Changes to the authorization, purpose, or signatory to the agreement all may be reasons that the agreement needs to be updated. The ASC's duties regarding information changes are detailed in Section **4.1.1**.

2) Authorized Personnel List (Section **4.1.2**)
   The ASC is responsible for maintaining an updated Authorized Personnel List on file with AZDPS. The APL contains those individuals whom the agency has identified as authorized to access, handle, and/or destroy CJI/CHRI. The authorizations are based solely on the agency's determination but should be limited to the minimum number of personnel necessary. All personnel who view, handle, use, disseminate, or dispose of CJI/CHRI must appear on the list; the list will be checked at every audit.

3) Agency File Information (Section **4.1.1**)
   The ASC should inform the Noncriminal Justice Compliance Team in writing of changes in the CEO, the ASC, or any relevant business information (agency name changes, mailing/physical address changes, etc.). The Compliance Specialist will check that all the information on file at DPS is current. Make changes as they occur – **Do not wait for an audit!**

4) Authorization and Purpose (Section **1.2**, Section **1.3**, Section **2.7.1**#17)
Each fingerprint submission access is for a specific purpose and is pursuant to a specific authorization. Fingerprints cannot be submitted for any purpose other than that which is named in the agency's authorization. Agencies may have more than one authorization, allowing them to submit fingerprints for multiple purposes. The Compliance Specialist will check all the agency's authorizations and verify each purpose.

A change to an agency's authorization may invalidate the entire user agreement; if the ASC becomes aware of a change in the authorization for access (e.g., change in the authorizing city ordinance, new state statute, etc.), he/she needs to contact the Access Integrity Unit immediately to update the user agreement and, if necessary, submit the new authorization to AZDPS for approval by the FBI.

5.2.2 Fingerprint Submissions

The Compliance Specialist will review the agency's entire fingerprint submission process covering properly filling out the cards, applicant identification, processes to protect the fingerprint card from tampering, and notifications and disclosures to the applicant.

1) Proper Citing of the "Reason Fingerprinted" (Section **2.7.1**#17)
Fingerprint cards can only be submitted for specific purposes under approved authorizations. In the "Reason Fingerprinted" box on the card, agencies are required to specify BOTH the particular purpose for the submission (employee, volunteer, license type) and the authorizing authority (statute number, city ordinance number, executive order number).

2) Applicant Identification (Section **2.2**)
Agencies should have processes for verifying the identity of the applicant at the time of fingerprinting. The Compliance Specialist will check for procedures which include:
   - Informing fingerprinting personnel of the identification requirement.
   - Requiring proper identification at the time of fingerprinting.

3) Protection of the Fingerprint Card Prior to Submission (Section **2.3**)
Agencies should have processes for protecting the integrity of the fingerprint card and preventing tampering with the card from the time the prints are taken through the submission to AZDPS. The Compliance Specialist will look for procedures that establish either a process that prevents the applicant from possessing a completed fingerprint card or prevents direct access to the card (such as a sealed envelope system). The processes should also include instructions for fingerprinting personnel as necessary.

4) Review and Challenge Notification (Section **3.3**)
It is the agency's responsibility to notify applicants of the opportunity and ability to review and challenge a criminal history record. Review and challenge contact information is in Section 3.3 of this guide.

5) FBI Applicant Privacy Rights Notifications (Section **2.5**)
Any agency which submits fingerprints for FBI criminal history (federal check) is required to advise applicants of the following before submitting the fingerprint card for a criminal history check:

   - Applicants must be notified in writing that their fingerprints will be used to check the criminal history records of the FBI. The written notification to the applicant must be

provided in a format where the applicant can read and take a copy with them if they desire.
- Informing all applicants that they are allowed a reasonable opportunity (this must be defined, i.e. 5 days) to complete and challenge the accuracy of the criminal history record before final denial.
- Agencies must notify applicants how to obtain a copy of the FBI record and that the guidelines for these procedures are contained in Title 28 Code of Federal Regulations 16.34.

Additionally:
- The agency should also establish and document what constitutes a reasonable time for the review and challenge and any appeals process that is available to the applicant.
- It is highly recommended (but not required) that the written notification be presented to the applicant on a document that the applicant is required to sign.

5.2.3 Privacy and Security

Agencies must have written policies and procedures regarding access, use, handling, dissemination, and destruction of CJI/CHRI (See section 3.1). The Compliance Specialist will review the agency's required privacy and security policies and procedures and any documents/processes related to the security and dissemination of CJI/CHRI. Section 3 of this guide covers the required policies and basic privacy and security guidelines.

1) The agency must have a process that ensures that CJI/CHRI is only used for the purpose for which it is requested.

2) The agency must have processes in place for the proper access and handling of CJI/CHRI.
    - Access includes:
        - Defining who is authorized to access CJI/CHRI
        - Restricting access to only Authorized Personnel
    - Handling rules include:
        - Proper security of CJI/CHRI from receipt through destruction
        - Communication rules
            - Communication among Authorized Personnel
            - Communication with the applicant concerning CJI/CHRI
        - Secondary dissemination procedures (if authorized)
            - Logging/tracking procedures
            - Procedures for authenticating recipients of the disseminated information
    - Retention procedures
    - Destruction procedures

3) The agency must have processes in place to prevent the unauthorized disclosure of CJI/CHRI. Prevention of unauthorized disclosure includes:
    - Access-limited storage.
    - Not leaving CJI/CHRI unattended when it is not physically secured.
    - Revocation of access privileges for terminated employees or those removed from the Authorized Personnel List.

4) The agency must have a formal disciplinary process in place for misuse of CJI/CHRI. If the agency has general misconduct or disciplinary policy, the agency would need to demonstrate how this policy would be applied/activated in the event of a misuse situation.

5) If applicable, the agency must have processes in place governing electronic storage of CJI/CHRI. This includes:
    - Monitoring and restricting access to databases containing CJI/CHRI.
    - Physical/technical safeguards to protect the access and integrity of the CJI/CHRI.
    - Reporting, response, and handling capability for information security incidents.

5.2.4 Training

The Compliance Specialist will review the agency's training documentation to check if Authorized Personnel have received both the mandatory CJIS Online training and the agency's internal process training. All personnel with access are required to be trained in the agency's internal privacy and security processes. Authorized Personnel do not need to attend AZDPS training; all required training takes place at the user agency.

1) All Authorized Personnel must be trained in the online security awareness (CJIS Online) training within six months of hire (or of being placed on the Authorized Personnel List) and then every two years thereafter.

2) All Authorized Personnel must receive the agency's internal training on the access/use/handling/dissemination/destruction procedures within six months of hire (or of being placed on the Authorized Personnel List) and then every two years thereafter. The agency's training should also cover the state, federal, and agency consequences for misuse of criminal history. The Compliance Specialist will ask to view the agency's training and any reference policies to assess the training topics. (See Section 4.2.1)

3) All Authorized Personnel must sign an Acknowledgement Statement acknowledging the notification of the penalties for misuse of CJI/CHRI. There is no standard format for the Acknowledgement Statement, but it must state at a minimum that the individual has been notified of the consequences of misuse of CJI/CHRI. Agencies may choose to summarize the consequences on the Acknowledgement Statement or refer to specific policies or training materials. (See Section 4.2.2)

4) Authorized Personnel training must be logged on the NCJ Training Documentation Form (or equivalent) and the documentation must be available for inspection by auditors.

Section 6 - DPS Classes & Assistance

AZDPS provides free training to noncriminal justice agencies receiving criminal justice information and criminal history record information. AZDPS's compliance training is designed to help the Agency Security Contact or other designated agency representative understand the compliance requirements so that they can implement the rules back at their agency; AZDPS training does not take the place of the user agency's internal training. It is each agency's responsibility to ensure that its authorized personnel are properly trained in the requirements detailed in Section 5.2.4.

Training reservations are first-come-first-serve and should be made by the ASC. To attend the training classes described in this subsection, the ASC should complete the *Training Reservation Form*, which can be found in Appendix H of this guide or at the AZDPS website. Please email NCJA@azdps.gov for the most current copy of the training calendar. **There are no fees for these classes**. Training courses are offered both online and in-person.

6.1 Initial Access & NCJ Compliance Training

All new agencies are required to have at least one representative attend Initial Access & NCJ Compliance Training before submitting any fingerprint cards. This training is not required for existing agencies; however, it is recommended if an agency has experienced personnel turnover or agency personnel wish to attend a refresher to ensure compliance with current requirements. The persons who attend training should be prepared to share the information learned with other relevant user agency personnel. This training is for the ASC and agency trainers – this is not the training which is required for all agency Authorized Personnel. Authorized Personnel training requirements are explained in the class. This class is also offered through our Microsoft Teams.

Class Description

Initial Access & NCJ Compliance Training lasts approximately three hours and covers the basic rules in this guide and provides information on the following:

- How to properly fill out the information on a fingerprint card and inventory sheet.
- Fingerprint submission packet requirements, including fees.
- How to read and interpret criminal justice information/criminal history record information.
- Complying with state and federal requirements associated with noncriminal justice fingerprint criminal history checks.
- Outlines the Agency Security Contact's role as the primary user agency liaison and guides user agency regulatory compliance and required documentation.
- Basic privacy and security guidelines for the access, use, handling, and destruction of criminal history record information.
- Advising agencies on the key areas they need to consider when developing policies and procedures for criminal history handling.
- Authorized personnel training requirements and an overview of CJIS Online Security Awareness training.

6.2 Additional Training Offered by AZDPS

The AZDPS AIU may offer other classes from time to time to address specific agency concerns or attempt to address the demand for a special type of refresher training. All current classes will appear on the training schedule and will be announced in the quarterly update email to the ASC.

To make reservations for a class, the ASC should use the Training Reservation Form. If the name of the class is not listed on the reservation form, fill in the name of the desired class in the blank next to "Other".

6.3 Obtaining Assistance from AZDPS

Please note that there are different AZDPS units involved in the fingerprint processes. The brief descriptions below may assist agencies in addressing questions to the appropriate unit. Please refer to page 4 of this guide for contact information for the AIU and the Applicant Team.

Access Integrity Unit Noncriminal Justice Compliance Team	**Applicant Team**
❖ Maintains user agency files and compliance documentation (processes access applications, Authorized Personnel Lists, information changes, and user agreements). ❖ Serves as a resource for CJI/CHRI privacy and security compliance. ❖ Coordinates New Fingerprint Accesses for agencies. ❖ Responsible for training user agencies (Initial Access & NCJ Compliance, special topics). ❖ Conducts noncriminal justice compliance audits.	❖ Processes incoming fingerprint card submissions from user agencies. ❖ Processes payments/fees for fingerprint submissions. ❖ Sends out the CJI/CHRI packets to user agencies. ❖ Processes requests for fingerprint cards and inventory sheet supplies. See Appendix I of this guide for the *Supply Order* form.

The AZDPS Applicant Clearance Card Team (ACCT) processes fingerprints for individuals submitting applications for a fingerprint clearance card. Please direct questions regarding clearance card processing to ACCT at (602) 223-2279.

References

The following state and federal sources referenced below contain rules, regulations, and policies governing the use and dissemination of criminal justice information and criminal history record information for noncriminal justice purposes. Most of these sources can be readily accessed online. This list is not exhaustive. Additional rules may also be contained in the specific authorization which allows the agency to access CJI/CHRI.

State of Arizona

Arizona Revised Statutes: http://www.azleg.gov/arstitle/

- A.R.S. § 41-1750 Central state repository; department of public safety; duties; noncriminal justice purposes: employment, licensing, volunteers, contract employees pursuant to authorization; review and challenge.
- A.R.S. §41-1756 Unauthorized access to criminal history; classification; definitions
- A.R.S. § 41-2204 System manager; power and duties
- A.R.S. § 41-2205 Criminal Justice information system central repository
- A.R.S. § 41-2206 Disciplinary action; system participants

Arizona Administrative Code Title 13: http://apps.azsos.gov/public_services/Title_13/13-01.pdf

Federal References

United States Code of Federal Regulations:
https://www.gpo.gov/fdsys/browse/collectionCfr.action?collectionCode=CFR

- Title 28 CFR § 20 Subpart C Federal System and Interstate Exchange of criminal history record information.
- Title 28 CFR §0.85(j) FBI authorized to approve procedures relating to the exchange of identification records.
- Title 28 CFR §50.12 Funds/approval for records exchange; dissemination limitations; required notification; review and challenge

United States Code: http://uscode.house.gov/search/criteria.shtml

- Title 5 U.S.C. § 552 Freedom of Information Act
- Title 5 U.S.C. § 552a Privacy Act of 1974 (as amended)
- Title 42 U.S.C. § 14616 Compact Council

Federal Bureau of Investigation: https://www.fbi.gov

- National Crime Prevention and Privacy Compact Council Compact Council Library: Resource documents and references by the Compact Council.
- Identity Verification Program Guide: Published by the National Crime Prevention and Privacy Compact Council to aid fingerprint-submitting agencies in developing policy, procedures, and practices for the positive identification of applicants.
- Federal Bureau of Investigations Criminal Justice Information Services (CJIS), CJIS Security Policy.

Acronym Glossary

ACIC	Arizona Criminal Information Center	State-level database containing records of stolen vehicles and wanted persons.
ACJIS	Arizona Criminal Justice Information System	Statewide network housing various databases of criminal justice information and criminal history record information.
AIU	Access Integrity Unit	Arizona Department of Public Safety unit that authorizes and monitors ACJIS usage and access.
A.R.S.	Arizona Revised Statutes	The Arizona laws enacted by the State Legislature. The most updated version can be found online at http://www.azleg.gov/arstitle/
ASC	Agency Security Contact	An individual assigned by their agency to act as a liaison between their agency and the Arizona Department of Public Safety. The responsibilities of the ASC are outlined in the user agreement and further explained in this manual.
CEO	Chief Executive Officer	The administrative head of the noncriminal justice agency/organization – typically the person with the power to sign legal contracts such as the user agreement.
CHRI	Criminal History Record Information	A particular subset of CJI. Defined in Arizona statute as "information that is collected by criminal justice agencies on individuals and that consists of identifiable descriptions and notations of arrests, detentions, indictments and other formal criminal charges, and any disposition arising from those actions, sentencing, formal correctional supervisory action, and release."
CJI	Criminal Justice Information	All state and federal criminal justice information system data, including fingerprint-based information. The use and dissemination of CJI, including CHRI, is subject to federal laws, state statutes, and FBI regulations.
CJIS	Criminal Justice Information Services	The division of the FBI that issues the security policy for the creation, viewing, modification, transmission, dissemination, storage, and destruction of criminal justice information.
CSA	CJIS Systems Agency	The state agency which is the main receiving point through which agencies in the state access systems are managed by the FBI CJIS Division. The CSA in Arizona is the Department of Public Safety.
CSO	CJIS Systems Officer	The person from the CSA who is responsible for ensuring the state's users comply with all applicable rules, laws, and regulations governing the use of the ACJIS/NCIC network.
CSR	Central State Repository	The agency responsible for collecting, maintaining, and disseminating criminal history records in Arizona. It is located in the AZDPS headquarters in Phoenix.
AZDPS	Arizona Department of Public Safety	State-level law enforcement agency protecting the property and citizens of Arizona. AZDPS also operates the Arizona CSA.

FBI	Federal Bureau of Investigation	The agency within the Department of Justice which encompasses the Criminal Justice Information Services (CJIS) Division.
NCIC	National Crime Information Center	The federal-level network that houses various databases on persons and property.
NCJA	Noncriminal Justice Agency	For access to CJI/CHRI, a noncriminal justice agency is an organization or organizational subunit that primarily provides services for other than criminal justice purposes.
ORI/OCA	Originating Agency Identifier (XX_ _ _ _ _ _ _ -- goes in the "Your No. OCA" box on the card)	A nine-character, alphanumeric identifier assigned to a specific agency that allows access to CJI/CHRI. This identifier usually starts with "XX" for noncriminal justice organizations and is the number that goes in the "Your No. OCA" box on the fingerprint card.
SID	State Identification Number	A unique number assigned to an individual whose fingerprints have been submitted to the state after an arrest.
UCN	Universal Control Number (FBI Number)	A unique number assigned to an individual whose fingerprints have been submitted to the FBI after an arrest.

EXAMPLE

EXAMPLE FINGERPRINT VERIFICATION FORM

This form is an example only. Modify the instruction steps to reflect your agency's approved process and insert agency-specific requirements/instructions where needed. Steps should include a method to prevent the applicant from tampering with the finished card such as the sealed envelope system or having the technician retain the card for later mailing or pickup. Additional instructions to the applicant might include items such as being printed only at specific locations or cautions that the fingerprints will be rejected if the envelope has been unsealed.

FINGERPRINT VERIFICATION FORM

ATTENTION FINGERPRINT TECHNICIAN:
Please follow the instructions below for fingerprinting this applicant.

1. Please fill out or ensure that the applicant has filled out all the required boxes on the fingerprint card prior to taking the fingerprints.

2. Request a valid, unexpired government-issued photo ID from the applicant and compare the physical descriptors on the applicant's photo ID to the applicant and to the information on the fingerprint card.

3. Fill out the information in the boxes below. Please print clearly.

4. Once the prints have been taken, place the fingerprint card and this form into the envelope and seal it. Please write your name or identification across the edge of the seal. Return the sealed envelope to the applicant. *Do not give the applicant the fingerprint card without first sealing it inside the envelope.*

PRINT the following information:

Date	**Name of Applicant**
Name of Fingerprint Technician (PRINT):	
Fingerprint Technician's Agency/Company Name	
Type of Photo ID provided (check one): **____ Driver's License/MVD Issued ID** **____ Other (Please specify)** **____ Passport** **_____**	

Guidelines for Required FBI Notifications Of Applicant Privacy Rights

Agencies which submit fingerprints to receive FBI criminal history records are required to make certain notifications to applicants who are fingerprinted for noncriminal justice purposes.

Agencies must advise the person being fingerprinted of the following notifications PRIOR to submitting the fingerprint card to the FBI (via DPS).

- The person being fingerprinted must be notified in writing that the fingerprints will be used to check the criminal history records of the FBI. The written notification to these applicants must be provided in a format where applicants can read and take a copy with them if they desire. Simply stating that an applicant is subject to a "national background check" is NOT sufficient.
- Applicants must be informed that they are allowed a reasonable opportunity (you must define this time frame, i.e. 5 days) to complete and challenge the accuracy of the criminal history record. ALL applicants must be advised of this, not just those who dispute an employment/license denial.
- Agencies must notify applicants how to obtain a copy of the FBI record and that the guidelines for these procedures are contained in Title 28 CFR 16.34.

If the applicant elects to review/challenge the criminal history record, the agency must provide the person a reasonable period of time to do so before final denial. Agencies should establish documented processes for what constitutes a reasonable period of time and any appeals processes available to the applicant.
The sample language in the box below contains the required notifications and disclosures.

Your fingerprints will be used to check the criminal history records of the FBI.

If you have a criminal history record, the officials making a determination of your suitability for employment, license, or other benefit must provide you the opportunity to complete or challenge the accuracy of the information in the record. You should be afforded a reasonable amount of time (*you must define this time frame, i.e. 5 days*) to correct or complete the record (or decline to do so) before officials deny you employment, license, or other benefit based on information in the criminal history record.

The procedures for obtaining a change, correction, or updating of your FBI criminal history record are set forth in Title 28, Code of Federal Regulations (CFR), Sections 16.30 through 16.34. Information on how to review and challenge your FBI criminal history record can be found at www.fbi.gov under “Services” and then "Identity History Summary Checks" or by calling (304) 625-5590.

To obtain a copy of your Arizona criminal history in order to review/update/correct the record, you can contact the Arizona Department of Public Safety Criminal History Records Unit at (602) 223-2222 to obtain a fingerprint card and a Review and Challenge packet. Information on the review and challenge process can be found on the DPS website (www.azdps.gov).

NONCRIMINAL JUSTICE APPLICANT'S PRIVACY RIGHTS

As an applicant who is the subject of a national fingerprint-based criminal history record check for a noncriminal justice purpose (such as an application for employment or a license, an immigration or naturalization matter, security clearance, or adoption), you have certain rights which are discussed below. All notices must be provided to you in writing. [1] These obligations are pursuant to the Privacy Act of 1974, Title 5, United States Code (U.S.C.) Section 552a, and Title 28 Code of Federal Regulations (CFR), 50.12, among other authorities.

- **You must be provided an adequate written FBI Privacy Act Statement (dated 2013 or later) when you submit your fingerprints and associated personal information. This Privacy Act Statement must explain the authority for collecting your fingerprints and associated information and whether your fingerprints and associated information will be searched, shared, or retained. [2]**
- **You must be advised in writing of the procedures for obtaining a change, correction, or update of your FBI criminal history record as set forth at 28 CFR 16.34.**
- **You must be provided the opportunity to complete or challenge the accuracy of the information in your FBI criminal history record (if you have such a record).**
- **If you have a criminal history record, you should be afforded a reasonable amount of time to correct or complete the record (or decline to do so) before the officials deny you the employment, license, or other benefit based on information in the FBI criminal history record.**
- **If agency policy permits, the officials may provide you with a copy of your FBI criminal history record for review and possible challenge. If agency policy does not permit it to provide you a copy of the record, you may obtain a copy of the record by submitting fingerprints and a fee to the FBI. Information regarding this process may be obtained at https://www.fbi.gov/services/cjis/identity-history-summary-checks and https://www.edo.cjis.gov.**
- **If you decide to challenge the accuracy or completeness of your FBI criminal history record, you should send your challenge to the agency that contributed the questioned information to the FBI. Alternatively, you may send your challenge directly to the FBI by submitting a request via https://www.edo.cjis.gov. The FBI will then forward your challenge to the agency that contributed the questioned information and request the agency to verify or correct the challenged entry. Upon receipt of an official communication from that agency, the FBI will make any necessary changes/corrections to your record in accordance with the information supplied by that agency. (See 28 CFR 16.30 through 16.34.)**
- **You have the right to expect that officials receiving the results of the criminal history record check will use it only for authorized purposes and will not retain or disseminate it in violation of federal statute, regulation or executive order, or rule, procedure or standard established by the National Crime Prevention and Privacy Compact Council.[3]**

---

[1] Written notification includes electronic notification, but excludes oral notification.
[2] https://www.fbi.gov/services/cjis/compact-council/privacy-act-statement
[3] See 5 U.S.C. 552a(b); 28 U.S.C. 534(b); 34 U.S.C. § 40316 (formerly cited as 42 U.S.C. § 14616), Article IV(c); 28 CFR 20.21(c), 20.33(d) and 906.2(d).

Updated 11/6/2019

DERECHOS DE PRIVACIDAD DE SOLICITANTES - JUSTICIA, NO CRIMINAL

Como solicitante sujeto a una indagación nacional de antecedentes criminales basado en huellas dactilares, para un propósito no criminal (tal como una solicitud para empleo o una licencia, un propósito de inmigración o naturalización, autorización de seguridad, o adopción), usted tiene ciertos derechos que se entablan a continuación. Toda notificación se le debe proveer por escrito.[1] Estas obligaciones son de acuerdo al Privacy Act of 1974, Title 5, United States Code (U.S.C.) Section 552a, y Title 28 Code of Federal Regulations (CFR), 50.12, entre otras autorizaciones.

- **Se le debe proveer una Declaración de la Ley de Privacidad del FBI (con fecha de 2013 o más reciente) por escrito cuando presente sus huellas digitales e información personal relacionada. La Declaración de la Ley de Privacidad debe explicar la autorización para tomar sus huellas digitales e información relacionada y si se investigarán, compartirán, o retendrán sus huellas digitales e información relacionada.[2]**
- **Se le debe notificar por escrito el proceso para obtener un cambio, corrección, o actualización de su historial criminal del FBI según delineado en el 28 CFR 16.34.**
- **Se le tiene que proveer una oportunidad de completar o disputar la exactitud de la información contenida en su historial criminal del FBI (si tiene dicho historial).**
- **Si tiene un historial criminal, se le debe dar un tiempo razonable para corregir o completar el historial (o para rechazar hacerlo) antes de que los funcionarios le nieguen el empleo, licencia, u otro beneficio basado en la información contenida en su historial criminal del FBI.**
- **Si lo permite la política de la agencia, el funcionario le podría otorgar una copia de su historial criminal del FBI para repasarlo y posiblemente cuestionarlo. Si la política de la agencia no permite que se le provea una copia del historial, usted puede obtener una copia del historial presentando sus huellas digitales y una tarifa al FBI. Puede obtener información referente a este proceso en https://www.fbi.gov/services/cjis/identity-history-summary-checks y https://www.edo.cjis.gov.**
- **Si decide cuestionar la veracidad o totalidad de su historial criminal del FBI, deberá presentar sus preguntas a la agencia que contribuyó la información cuestionada al FBI. Alternativamente, puede enviar sus preguntas directamente al FBI presentando un petición por medio de .https://www.edo.cjis.gov. El FBI luego enviará su petición a la agencia que contribuyó la información cuestionada, y solicitará que la agencia verifique o corrija la información cuestionada. Al recibir un comunicado oficial de esa agencia, el FBI hará cualquier cambio/corrección necesaria a su historial de acuerdo con la información proveída por la agencia. (Vea 28 CFR 16.30 al 16.34.)**
- **Usted tiene el derecho de esperar que los funcionarios que reciban los resultados de la investigación de su historial criminal lo usarán para los propósitos autorizados y que no los retendrán o diseminarán en violación a los estatutos, normas u órdenes ejecutivos federales, o reglas, procedimientos o normas establecidas por el National Crime Prevention and Privacy Compact Council.[3]**

---

1 La notificación por escrito incluye la notificación electrónica, pero excluye la notificación verbal.
2 https://www.fbi.gov/services/cjis/compact-council/privacy-act-statement
3 Vea 5 U.S.C. 552a(b); 28 U.S.C. 534(b); 34 U.S.C. § 40316 (anteriormente citada como 42 U.S.C. § 14616), Article IV(c); 28 CFR 20.21(c), 20.33(d) y 906.2(d).

Privacy Act Statement

This privacy act statement is located on the back of the FD-258 fingerprint card.

Authority: The FBI's acquisition, preservation, and exchange of fingerprints and associated information is generally authorized under 28 U.S.C. 534. Depending on the nature of your application, supplemental authorities include Federal statutes, State statutes pursuant to Pub. L. 92-544, Presidential Executive Orders, and federal regulations. Providing your fingerprints and associated information is voluntary; however, failure to do so may affect completion or approval of your application.

Principal Purpose: Certain determinations, such as employment, licensing, and security clearances, may be predicated on fingerprint-based background checks. Your fingerprints and associated information/biometrics may be provided to the employing, investigating, or otherwise responsible agency, and/or the FBI for the purpose of comparing your fingerprints to other fingerprints in the FBI's Next Generation Identification (NGI) system or its successor systems (including civil, criminal, and latent fingerprint repositories) or other available records of the employing, investigating, or otherwise responsible agency. The FBI may retain your fingerprints and associated information/biometrics in NGI after the completion of this application and, while retained, your fingerprints may continue to be compared against other fingerprints submitted to or retained by NGI.

Routine Uses: During the processing of this application and for as long thereafter as your fingerprints and associated information/biometrics are retained in NGI, your information may be disclosed pursuant to your consent, and may be disclosed without your consent as permitted by the Privacy Act of 1974 and all applicable Routine Uses as may be published at any time in the Federal Register, including the Routine Uses for the NGI system and the FBI's Blanket Routine Uses. Routine uses include, but are not limited to, disclosures to: employing, governmental or authorized non-governmental agencies responsible for employment, contracting, licensing, security clearances, and other suitability determinations; local, state, tribal, or federal law enforcement agencies; criminal justice agencies; and agencies responsible for national security or public safety.

As of 03/30/2018

See Page 2 for Spanish translation.

Declaración de la Ley de Privacidad

Esta declaración de la ley de privacidad se encuentra al dorso del FD-258 tarjeta de huellas digitales.

Autoridad: La adquisición, preservación, e intercambio de huellas digitales e información relevante por el FBI es autorizada en general bajo la 28 U.S.C. 534. Dependiendo de la naturaleza de su solicitud, la autoridad incluye estatutos federales, estatutos estatales de acuerdo con la Pub. L. 92-544, Órdenes Ejecutivas Presidenciales, y reglamentos federales. El proveer sus huellas digitales e información relevante es voluntario; sin embargo, la falta de hacerlo podría afectar la terminación o aprobación de su solicitud.

Propósito Principal: Ciertas determinaciones, tal como empleo, licencias, y autorizaciones de seguridad, podrían depender de las investigaciones de antecedentes basados en huellas digitales. Se les podría proveer sus huellas digitales e información relevante/ biométrica a la agencia empleadora, investigadora, o responsable de alguna manera, y/o al FBI con el propósito de comparar sus huellas digitales con otras huellas digitales encontradas en el sistema Next Generation Identification (NGI) del FBI, o su sistema sucesor (incluyendo los depósitos de huellas digitales latentes, criminales, y civiles) u otros registros disponibles de la agencia empleadora, investigadora, o responsable de alguna manera. El FBI podría retener sus huellas digitales e información relevante/biométrica en el NGI después de terminar esta solicitud y, mientras las mantengan, sus huellas digitales podrían continuar siendo comparadas con otras huellas digitales presentadas a o mantenidas por el NGI.

Usos Rutinarios: Durante el procesamiento de esta solicitud y mientras que sus huellas digitales e información relevante/biométrica permanezcan en el NGI, se podría divulgar su información de acuerdo a su consentimiento, y se podría divulgar sin su consentimiento de acuerdo a lo permitido por la Ley de Privacidad de 1974 y todos los Usos Rutinarios aplicables según puedan ser publicados en el Registro Federal, incluyendo los Usos Rutinarios para el sistema NGI y los Usos Rutinarios Generales del FBI. Los usos rutinarios incluyen, pero no se limitan a divulgación a: agencias empleadoras gubernamentales y no gubernamentales autorizadas responsables por emplear, contratar, licenciar, autorizaciones de seguridad, y otras determinaciones de aptitud; agencias de la ley locales, estatales, tribales, o federales; agencies de justicia penal; y agencias responsables por la seguridad nacional o seguridad pública.

A partir de 30/03/2018

ARIZONA DEPARTMENT OF PUBLIC SAFETY
APPLICANT TEAM

P.O. Box 18430 Phoenix, Arizona 85005-8390
Telephone (602) 223-2223 Fax (602) 223-2972

DOUGLAS A. DUCEY
Governor

COLONEL HESTON SILBERT
Director

STATE AGENCY SUBMISSION SHEET

IETAT AFIS TRANSFERS ONLY FOR THE APPLICANT TEAM.

Please fill out all of the information listed below:

Agency Name: _____ **ORI** _____

AFIS Document IETAT ID #: _____

AFIS Transaction Submission Date: _____

Total # of fingerprints Submitted: _____

Total Transaction Amount Transferred: _____

Prepared By: _____

Date: _____

Phone #: _____

Inventory Sheet Numbers:

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

Revised on February 23, 2017

CJIS NAME SEARCH REQUEST FORM

Please complete the attached form to request a name check. A name search will not be conducted unless an individual's fingerprints have been rejected twice for technical issues.

ORI of State/Federal/Regulatory Agency: AZDPS2000

Your agency's Point of Contact (POC) for the response: **ZEE JONES**

Phone number of POC: (602) 223-2722

Fax number of POC: (602) 223-2972

Address of requesting agency: AZ DPS (AZAFIS OPERATIONS)
2222 W ENCANTO BLVD
PHOENIX, AZ 85005-6638

Please fax my response to this request to the POC @ 602-223-2972.

Subject of Name Check

Control Number (PCN) of subject's fingerprint submission: **2A**_____
(bar code number) **2A**_____

Name: _____ **Alias:** _____

Date of Birth: _____ Place of Birth: _____

Social Security Number: _____

OCA#: _____

Requesting Agency: _____

(DPS use only)
Date faxed to DPS: _____ Date faxed to FBI:_____

*** BOLDED FIELDS REQUIRED**

Arizona Department of Public Safety
Noncriminal Justice Agency *Information Change* Form

Date	**Agency Name**	**Agency ORI/OCA** ("XX" identifier)

Change/Add Contact Type: Check all that apply Agency Security Contact (ASC) ☐ Applicant Team ☐ Secondary ASC ☐	***Previous* Contact**		
	New Contact Information		
	Title	**Name**	
	Phone	**Fax**	**Email**

Change CEO	***Previous* CEO Name**		
	New CEO Information		
	Title	**Name**	
	Phone	**Fax**	**Email**

Change Address Type: Physical ☐ Mailing ☐ Both ☐	**Address Line 1**		
	Address Line 2		
	City	**State**	**Zip**

Change Agency Name Previous Name: New Name:	**Change Agency Main Phone** New phone number:

Additional Comments/Information:	Leave Blank – AIU use only
Name and Title of Person Submitting Form (Please Print Legibly):	

Send completed form to:

Arizona Department of Public Safety
Access Integrity Unit
ATTN: Noncriminal Justice Compliance
P.O. Box 6638 | MD 3160
Phoenix, AZ 85005-6638

OR

Fax: (602) 223-2926
ATTN: AIU Noncriminal Justice Compliance

Email: NCJA@azdps.gov

EXAMPLE AUTHORIZED PERSONNEL LIST

Earth Traditional Academy

10200 Terra Grande Ln
Grand Ol Planet, AZ 86000

Keeping your children
firmly planted

June 30, 2015

Arizona Department of Public Safety
Access Integrity Unit
Noncriminal Justice Compliance Team
P.O. Box 6638 | MD 3160
Phoenix, AZ 85005-6638

Dear Noncriminal Justice Compliance Team:

The following is an updated authorized personnel list for the Earth Traditional Academy.

Authorized Individual	**Title**
Jane Smith	HR Director
Tim Farris	Plans & Policy
Debra Mattis	Administrative Assistant
Adam Ricker (ASC)	Director
Sandy Mills	Receptionist

If you have any questions, you can reach me at (800) 500-5000 Ext 1.

Sincerely,

Adam Ricker

Adam Ricker
Agency Security Contact
Human Resources Director, Earth Traditional Academy

EXAMPLE

NONCRIMINAL JUSTICE AGENCY TRAINING DOCUMENTATION FORM

AGENCY NAME:_____ **ORI/OCA:**_____

The following 2 types of training are REQUIRED.
completed within 6 months of hire or appointment to position with access to criminal justice/criminal history record information. Refresher training must be repeated every two years for as long as the individual is on the agency Authorized Personnel List and granted access to criminal justice and/or criminal history record information.
Security Awareness Training - via www.CJISOnline.com. Provides a generic base-level overview of CJI/CHRI security.
Agency Internal Privacy and Security Training - Internal agency training on the agency's security and handling processes prior to being allowed access to criminal justice and/or criminal history record information.

Name	First Time (F) or Refresher Training (R)?	Date of Security Awareness Training (CJIS online)	Date of Agency Privacy & Security Training	Acknowledgement Statement Signed? (Y/N)
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				

The persons named above have received the required training in accordance with applicable rules and regulations.

ASC Printed Name: _____ ASC Signature: _____ Date:_____

PLEASE PRINT LEGIBLY- Keep training logs on file. Training logs will be reviewed during audits. The Arizona Department of Public Safety (DPS) will also periodically request the agency submit training logs as part of quality assurance and compliance review. Please do not send training logs to DPS unless requested.

Arizona Department of Public Safety
Noncriminal Justice Agency Training Reservation Form

The Department of Public Safety Access Integrity Unit (AIU) offers training classes to assist noncriminal justice agencies which submit applicant fingerprint cards in maintaining compliance with state and federal law as it pertains to accessing criminal justice and criminal history record information. Descriptions of the basic classes can be found in the DPS Classes & Assistance section of the Arizona Noncriminal Justice Agency Guide. Classes are held once a month, via on-line training through the Microsoft Teams application and/or in the Phoenix classroom. Classes are free of charge and are subject to cancellation for low enrollment.

To make reservations for training, the Agency Security Contact (ASC) should fill out form, and indicate the class and training date requested, and return it to AIU. Confirmation will be emailed to the ASC.

Training Reservation Form		
Agency Name	**Agency OCA** **XX_____**	**Today's Date**
Agency Security Contact Name	**Agency Security Contact Phone**	
Agency Security Contact Email		
Please list all attendees and their email addresses. We will email important check-in information and directions.		

	Class Name	**Training Date**	**# of Attendees**
_____	**Initial Access & NCJ Compliance Training (Required for new agencies)**	_____	_____
_____	**ONLINE - Initial Access & NCJ Compliance Training (Required for new agencies)**	_____	_____
_____	**Other:**	_____	_____

Send completed form to: Compliance

Arizona Department of Public Safety
Access Integrity Unit
ATTN: Noncriminal Justice Compliance
P.O. Box 6638 | MD 3160
Phoenix, AZ 85005-6638

OR

Fax: (602) 223-2926
ATTN: AIU Noncriminal Justice

Email: NCJA@azdps.gov
Subject line: Training Reservation

ORDERING ***APPLICANT TEAM*** SUPPLIES

PLEASE COMPLETE THIS FORM AND FAX OR MAIL TO:

Arizona Department of Public Safety
Applicant Team
Mail Drop 3190
P.O. Box 18430
Phoenix, AZ 85005-8430

PHONE: (602) 223-2223
FAX: (602) 223-2972

ITEM	AMOUNT REQUESTED
Applicant Fingerprint Cards 2000/box	_____
Inventory Sheet (802-06513) 250/pack (For non-criminal justice purposes)	_____

Agency Name: _____

Agency ORI: _____

Address: _____

_____

_____

Telephone #: _____

Order Date: _____

PLEASE ALLOW 1-2 WEEKS FOR PROCESSING OF ORDER