ARIZONA NONCRIMINAL JUSTICE COMPLIANCE PROGRAM

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

Arizona Department of Public Safety
Access Integrity Unit
August 2015

Table of Contents

Introduction		**3**
Contact List		**4**
Section 1 General Overview		
1.1	DPS Overview	**5**
1.2	User Agreement	**5**
1.3	Authorizations and Access	**6**
	1.3.1 Application for Access	**6**
	1.3.2 New Authorizations	**6**
	1.3.3 Criminal Justice versus Noncriminal Justice Accesses	**6**
Section 2 Fingerprint Submissions & Results		
2.1	Arizona Fingerprinting Processes	**7**
	2.1.1 Fingerprint Clearance Card Process	**7**
	2.1.2 Fingerprint Criminal History Check Process	**7**
	2.1.3 Fingerprint Processes Chart	**8**
2.2	Applicant Identification	**8**
2.3	Protection of the Fingerprint Card Prior to Submission	**9**
2.4	Identity-Verified Prints Process for IVP Clearance Cards (Schools Only)	**10**
2.5	FBI Applicant Privacy Rights Notifications	**10**
2.6	Basic Fingerprinting Tips	**10**
2.7	Required Information for Each Fingerprint Card	**12**
	2.7.1 Fingerprint Card Legend	**12**
2.8	Example Fingerprint Cards	**15**
2.9	Inventory Sheet	**17**
	2.9.1 Inventory Sheet Legend	**17**
	2.9.2 Inventory Sheet and Distribution	**17**
2.10	Payment and Submission Packets	**19**
	2.10.1 Fees	**19**
	2.10.2 Payment Submittal Requirements	**19**
	2.10.3 Submission Packet	**19**
2.11	Rejected Fingerprint Cards/Resubmissions	**20**
	2.11.1 Name Searches on FBI Rejects	**20**
	2.11.2 Routine Name Search Procedure	**21**
2.12	DPS Results	**22**
2.13	FBI Results	**28**
Section 3 Basic Privacy and Security Guidelines		
3.1	Policies and Procedures	**34**
3.2	Applicant Process	**35**
3.3	Applicant Review and Challenge of Criminal History	**35**
3.4	Communication/Dissemination	**35**

3.4.1	Communication Cautions	**35**
3.4.2	Secondary Dissemination	**36**
3.5	Physical Security	**36**
3.5.1	Storage	**36**
3.5.2	Destruction	**37**
3.6	Technical/Digital Security	**37**
3.7	Consequences for Misuse	**38**
	Section 4 ASC Responsibilities	
4.1	Primary Liaison	**39**
4.1.1	Information Changes	**39**
4.1.2	Authorized Personnel List	**40**
4.2	Privacy and Security Coordinator	**40**
4.2.1	Required Training for Authorized Personnel	**40**
4.2.2	Acknowledgement Statements	**41**
4.3	Audit Responsibilities	**41**
	Section 5 Audits & Compliance	
5.1	Audits	**42**
5.1.1	Routine Audits	**42**
5.1.2	Directed Audits	**42**
5.2	Compliance Review	**43**
5.2.1	General Administration	**43**
5.2.2	Fingerprint Submissions	**44**
5.2.3	Privacy and Security	**45**
5.2.4	Training	**46**
	Section 6 DPS Classes & Assistance	
6.1	Initial Access Training	**47**
6.2	NCJA Compliance Training	**47**
6.3	Additional Training Offered by DPS	**48**
6.4	Obtaining Assistance from DPS	**48**
References		**49**
Acronym Glossary		**50**
Appendix A	Applicant Team Supplies Order Form	
Appendix B	FBI Name Search Request (Instructions B-1, Form B-2)	
Appendix C	Example Authorized Personnel List	
Appendix D	Noncriminal Justice Agency Information Change Form	
Appendix E	Noncriminal Justice Agency Training Documentation Form	
Appendix F	Noncriminal Justice Agency Training Reservation Form	
Appendix G	Example Fingerprint Verification Form	

Introduction

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

Public Law 92-544, passed by Congress in October 1972, 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 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 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.

In Arizona, ARS (Arizona Revised Statute) §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 (DPS) is the CSA for Arizona and also operates the central state repository which collects, maintains, and disseminates criminal history in Arizona. ARS §41-1750 also provides state authorizations for 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, provide guidance regarding 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

Available Monday through Friday from 8:00am to 5:00pm. Closed on state and federal holidays.

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

Arizona Department of Public Safety Applicant Team – MD 2250 P.O. Box 18430 Phoenix, AZ 85005-8430	Supervisor - Christopher Ramsey Phone: (602) 223-2722 Email: cramsey@azdps.gov

AUDITS, TRAINING, and PRIVACY & SECURITY

Department: Access Integrity Unit

Available Monday through Friday from 8:00am to 4:00pm. Closed on state and federal holidays.

Noncriminal Justice Compliance Team

Phone: (602) 223-2720 or (602) 223-2327

Email: NCJA@azdps.gov

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

Website: www.azdps.gov/Services/NCJA

Arizona Department of Public Safety Access Integrity Unit - MD 1190 ATTN: Noncriminal Justice Compliance P.O. Box 6638 Phoenix, AZ 85005-6638	Supervisor phone: (602) 223-2488 Email: accessintegrity@azdps.gov (please specify "For Supervisor" in the subject line

Section 1 - General Overview

1.1 DPS Overview

The Arizona Department of Public Safety (DPS) houses the Central State Repository (CSR) and is the state agency responsible for collecting, maintaining, and disseminating criminal history records in Arizona. DPS 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 information system that provides authorized Arizona agencies with various types of record information such as criminal history, Sex Offender Registration, 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 in order to maintain the integrity of the system and its records. Within DPS, the Access Integrity Unit (AIU) performs several duties in regard to 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 use of system information
- Monitoring system access and researching/investigating security breaches

The Noncriminal Justice Compliance Team is a part of the Access Integrity Unit.

The DPS Applicant Team processes the fingerprint cards and associated payments, and returns the criminal history check results to the submitting agency via mail.

1.2 User Agreement

Each agency authorized to receive criminal justice information (CJI) and criminal history record information (CHRI) must sign a user agreement. A user agreement is a contractual agreement between the authorized receiving organization and DPS; it must be signed by both the Arizona CSO and the appropriate authority at the user agency. (DPS refers to that agency authority as the Chief Executive Officer [CEO].) 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 authorization granting access to the information. **It is prohibited for noncriminal justice agencies to use criminal justice information (CJI) and criminal history record information (CHRI) for any purpose other than that for which it was requested.**

- Sanctions/Penalties: The user agreement is subject to cancellation by either party with 30 days written notice. DPS reserves the right to suspend service for violations or for 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 DPS. The responsibilities of the ASC are covered in Section 4.

- Training: Agencies are responsible for mandatory training requirements. New agencies opening a fingerprint access must attend Initial Access Training at DPS prior to submitting cards. Existing agencies are not required to attend training at DPS; however, 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.

1.3 Authorizations and Access

Each noncriminal justice access must be authorized by a specific statute, ordinance, or executive order. Agencies which desire to open a new access to submit fingerprints must submit an application to DPS.

1.3.1 Application for Access

Prior to submitting fingerprint cards and receiving criminal history information, a new user agency must complete an application for access, sign a user agreement, and attend Initial Access Training. For the application to be approved, there must be an authorization in place in order to open that access; the authorization must be cited on the application. Applications are available for download on the DPS website in the Public Services section under NCJA Fingerprint Compliance. Applications are reviewed by the DPS Access Integrity Unit. If approved, AIU will send out a user agreement and information regarding the additional steps to be completed to establish the access.

New agencies must also attend Initial Access Training at DPS. The training is designed to assist the agency in carrying out its responsibilities under the user agreement and maintaining compliance with laws and regulations. Once initial requirements are met, the agency is issued an ORI or OCA, which is a nine character alphanumeric identifier beginning with "XX"; this number is the agency's submission access number for fingerprint criminal history checks. Fingerprint cards and inventory sheets are provided by DPS free of charge.

1.3.2 New Authorizations

New authorizations (such as new city ordinances) must be submitted to DPS for approval before any access applications for the new purpose will be approved. If the fingerprints will be used to check both state and FBI records, then DPS will also submit the authorization to the FBI for approval. DPS can assist agencies with the appropriate verbiage which must be included in the authorization in order to obtain approval from the FBI. If there are any changes to the authorization at a later date, it must be resubmitted for approval (i.e., the authorization is a city ordinance and that ordinance is later superseded).

1.3.3 Criminal Justice versus Noncriminal Justice Accesses

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 must be submitted with a noncriminal justice ORI/OCA in order to obtain criminal history checks for noncriminal justice purposes; "running" III checks is not permitted. 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 regarding the types of access, please contact the Access Integrity Unit.

Section 2 - Fingerprint Submissions & Results

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

- Understanding the fingerprinting processes in Arizona
- Using quality assurance procedures for applicant identity verification and fingerprint card tampering prevention
- Comply 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 Fingerprinting Processes

There are two fingerprinting processes in Arizona: the fingerprint clearance card process and the fingerprint criminal history check process. The subsections below explain the difference in the two processes. Please note that this guide concentrates on fingerprint submissions and compliance rules for the fingerprint criminal history check process.

2.1.1 Fingerprint Clearance Card Process

The fingerprint clearance card process occurs between an individual applicant and DPS, not an agency. In order to apply for a fingerprint clearance card, the individual MUST fall into one of the categories listed on either the IVP (Identity-Verified Prints) 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 Department of Education teacher certification or foster care licensure through the Department of Child Safety. Eligibility to apply for a clearance card is NOT based solely on contact with children; it is based on falling into a specific category of certification/licensure or employment/volunteer designated in state statute. At this time, 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 to DPS for a clearance card, DPS checks the same state/FBI databases that are checked in the fingerprint criminal history check process. This application process is between the individual and DPS; an agency may facilitate the application process by supplying instructions and applications, but the process does not fundamentally involve the agency. DPS reviews the criminal history and makes the suitability determination based on the precluding factors set out in state law; the agency the person works does not receive a copy of the criminal history record. The plastic 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 for any subsequent private correspondence related to the clearance card, applicants should put their own 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 Arizona Revised Statutes (ARS) 41-1758.03 and ARS 41-1758.07. Subsequent Arizona arrests/convictions may result in a "file stop" and trigger a review to see if a clearance card should be suspended or revoked. The clearance card is the property of the individual; any agency may make a copy of it but must return it to the individual.

2.1.2 Fingerprint Criminal History Check Process

In the fingerprint criminal history check process, the agency has a legal authorization to submit applicant fingerprints to DPS. The process takes place between the agency and DPS; the agency sends in the prints and the available criminal history record is sent to the agency for review. If there is no criminal history, the DPS and/or FBI Results Report will indicate a negative response. The use of the 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 DPS and is subject to compliance regulations and periodic audit.

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 DPS. 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 clearance card determination.

2.1.3 Fingerprint Processes Chart

CRIMINAL HISTORY CHECK VS. CLEARANCE CARD		
Feature	**Fingerprint Criminal History Check**	**Fingerprint Clearance Card**
Arizona & FBI fingerprint criminal history databases checked	Yes - (unless agency authorization is for state criminal history only)	Yes
Plastic card issued	No	Yes - expires in 6 years (unless suspended or revoked)
Full CHRI results reviewed by employing/licensing agency	Yes	No - DPS 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 - authorization is specific to 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 DPS 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.

The National Crime Prevention and Privacy 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 website in the Compact Council section. Compact Council recommendations regarding proper identification of applicants include:

- Accept only valid, unexpired photo identification documents as primary proof of identity.
- 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 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 contracts with an outside agency for fingerprinting, then the agency should provide the contractor with specific guidance on identifying an applicant. If an applicant is allowed to go to various locations, then instructions should be provided to the applicant to give to the fingerprint technician. To ensure the instructions are followed, it is recommended that the instruction form require 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 documents the type of photo identification presented by the applicant.
- Establish procedures that use specially 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 given a 9x12 brown mailing envelope containing a fingerprint card and a "Fingerprint Verification Form" which contain instructions and a section which must be filled out by the fingerprint technician. The instructions tell 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 tell the fingerprint technician to put 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.

There is an example "Fingerprint Verification Sheet" sheet in Appendix G of this manual and on the DPS website in the NCJA Fingerprint Compliance section.

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 DPS identity-verified fingerprints process for IVP Clearance Cards.

Identity-verified fingerprints may be done 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 card. The fingerprint technician should mail the IVP application, card, and payment to DPS in the postage-paid envelope. To maintain the required chain-of-custody for the fingerprint card, the applicant may not be allowed to handle or take the fingerprint card with them after the fingerprints are on it.

A copy of *Guidelines for Identity-Verified Prints* is on the DPS website under NCJA Fingerprint Compliance.

2.5 FBI Applicant Privacy Rights Notifications

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 the 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 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.
- The person being fingerprinted must be informed that they are allowed a reasonable opportunity 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 period of time to do so before final denial.
    - The agency should also establish and document what constitutes a reasonable period of time for the review and challenge and any appeals process that is available to the applicant.
- Agencies must notify applicants how to obtain a copy of the FBI record and that the guidelines for these procedures are contained in 28 CFR 16.34.

A copy of the *Guidelines for Required FBI Notifications of Applicant Privacy Rights* can be found on the DPS website in the NCJA Fingerprint Compliance section.

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. The tips here should get you started, and then all you need is practice.

DPS 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 prior to 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 prior to 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 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 nail edge to 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 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 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 residence 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 OPERTNS 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 No. OCA**: 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

11. **Race**: Enter the one letter abbreviation for 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 person's eye and hair color.

EYE COLOR		HAIR COLOR	
BLK	Black	**BLK**	Black
BRO	Brown	**BRO**	Brown
GRN	Green	**BLN**	Blond or "strawberry"
MAR	Maroon	**RED**	Red or auburn
PNK	Pink	**SDY**	Sandy
BLU	Blue	**GRY**	Gray
GRY	Gray	**WHT**	White
HAZ	Hazel	**BLU**	Blue
MUL	Multi-colored	**ONG**	Orange
		PNK	Pink
		PLE	Purple
		BLD	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 which 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 proper box for each finger:**
    - A complete set of inked fingerprint impressions must be submitted.

    - Fingerprints must be rolled from side of nail to side of 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 proper 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

APPLICANT

LEAVE BLANK

TYPE OR PRINT ALL INFORMATION IN BLACK

LAST NAME NAM FIRST NAME MIDDLE NAME

LAST NAME FIRST NAME MIDDLE

FBI LEAVE BLANK

SIGNATURE OF PERSON FINGERPRINTED

SIGNATURE OF APPLICANT

ALIASES AKA

OTHER NAMES

INCLUDING MAIDEN

ORI

AZDPS2000
DPS-AFIS OPERATIONS
PHOENIX, AZ

RESIDENCE OF PERSON FINGERPRINTED

STREET ADDRESS

CITY, STATE, ZIP

DATE OF BIRTH DOB Month Day Year

MM/DD/YYYY

CITIZENSHIP CTZ

SEX SEX | RACE RACE | HGT HGT | WGT WGT | EYES EYE | HAIR HAIR | PLACE OF BIRTH POB STATE

DATE DATE | SIGNATURE OF OFFICIAL TAKING FINGERPRINTS FINGERPRINT TECH NAME/ID #

YOUR NO. OCA

YOUR AGENCY'S ORI/OCA

FBI NO. FBI

LEAVE BLANK

CLASS

REF.

EMPLOYER AND ADDRESS

NAME OF AGENCY
MAILING ADDRESS
CITY, STATE ZIP

ARMED FORCES NO. MNU

REASON FINGERPRINTED

REASON FOR SUBMISSION

STATUTORY AUTHORITY

SOCIAL SECURITY NO. SOC

SOCIAL SECURITY #

MISCELLANEOUS NO. MNU

INVENTORY SHEET #

➔ **ROLL PRINTS**

Right thumb	1	Right middle finger	Right ring finger	Right little finger
1. R. THUMB	2. R. INDEX	3. R. MIDDLE	4. R. RING	5. R. LITTLE

➔ **ROLL PRINTS**

Left thumb	Left index finger	Left middle finger	Left ring finger	Left little finger
6. L. THUMB	7. L. INDEX	8. L. MIDDLE	9. L. RING	10. L. LITTLE

➔ **PRESS PRINTS FLAT**

Left four fingers taken at the same time	Left thumb	Right thumb	2
LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY	L. THUMB	R. THUMB	RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY

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 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: BEAR
FIRST NAME: FUZZY
MIDDLE NAME: DE

FBI LEAVE BLANK

SIGNATURE OF PERSON FINGERPRINTED: Fuzzy De Bear

ALIASES AKA: FUZZY DONLIKE
BEAR, REBEL

ORI: AZDPS2000
DPS-AFIS OPERATIONS
PHOENIX, AZ

RESIDENCE OF PERSON FINGERPRINTED:
1 LIVE ERE STREET
HIBERNATE, AZ 85000

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

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: Ibe Tekperson

YOUR NO. OCA: XX000000E

LEAVE BLANK
CLASS
REF.

EMPLOYER AND ADDRESS:
WE LOVE EVERYONE
1 WORKING DERE AVE
NEXTTOHIBERNATE, AZ 85000

FBI NO. FBI

ARMED FORCES NO. MNU

REASON FINGERPRINTED:
EMPLOYEE
ARS 41-1750

SOCIAL SECURITY NO. SOC: 123-45-6789

MISCELLANEOUS NO. MNU: 271300

1. R. THUMB
2. R. INDEX
3. R. MIDDLE
4. R. RING
5. R. LITTLE
6. L. THUMB
7. L. INDEX
8. L. MIDDLE
9. L. RING
10. L. LITTLE

Left four fingers taken simultaneously

L. THUMB
R. THUMB

RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY

2.9 Inventory Sheet

An inventory sheet must be submitted each time fingerprint cards are sent to DPS. 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.

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 sheets. (Example: Use one 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 last name. A maximum of 30 applicants can be listed on one inventory sheet. Use a separate inventory sheet for additional applicants or for different types of applicants.

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

2.9.2 Inventory Sheet and 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. Please retain the agency copy until the agency's next noncriminal justice routine compliance audit to allow for review and verification of submissions.

ARIZONA DEPARTMENT OF PUBLIC SAFETY

NON-CRIMINAL JUSTICE APPLICANT FINGERPRINT CARD INVENTORY SHEET

Inventory Sheet Number
271300

Applicant Team ☎ **(602) 223-2223**

Applicant Team
Mail Drop 2250
P.O. Box 18430
Phoenix, AZ 85005-8430

Date	Submitting Agency's Name	Submitting Agency's ORI/OCA Number
3/6/2015	*We Love Everyone*	*XX000000E*

Type of Applicant(s) (Check One Box Only)
- ☐ **Regular Applicants**
- ☐ **Resubmits** (No Fee Required)
- ☐ **Volunteers**
- ☐ **State Level Only**

Direct Phone Number of Contact Person
(555) 555-5555

	Applicant's Name	Date of Birth
1	Bear, Fuzzy De	10/18/1982
2	Kenobi, Ben	09/23/1937
3	Skywalker, Luke	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

- ☐ ↑ **Fill out the top portion of this inventory sheet with your agency's information.** ***All fields are required.***
- ☐ ↖ **Check the box that corresponds to the type of applicant(s) being submitted with this sheet.** Only *one* type of applicant can be submitted per inventory sheet. If you have a mix of regular applicants, volunteers, resubmits and/or state level only applicants they ***must*** be submitted with separate inventory sheets with separate payment for each type of applicant.
- ☐ ← ***Print*** **the names and dates of birth of the applicant(s) being submitted with this sheet in the spaces on the left in alphabetical order.** 1 to 30 applicants may be submitted per inventory sheet.
- ☐ ↗ **Write the Inventory Sheet Number from the top right corner of this form in the "Miscellaneous No" box on all applicant fingerprint card(s) being submitted with this sheet.** Only blue lined "applicant" fingerprint cards should be submitted to Applicant Team One. ***Do not*** submit pre-printed fingerprint cards meant for any other purpose (e.g. the "Fingerprint Clearance Card" fingerprint cards). ***Do not*** submit prints on white (crime scene), green lined (personal ID) or red/pink lined (arrest) fingerprint cards. ***Do not*** submit bent, stapled, stained or otherwise altered fingerprint cards.
- ☐ ← **Enclose payment in the *exact* amount required for the number of applicant(s) being submitted.** If the amount is not exact it will be rejected. No payment is required for resubmits. A maximum of three forms of payment can be accepted per inventory sheet (e.g. two money orders and a cashier's check). You may provide one form of payment for up to 35 inventory sheets as long as only one type of applicant is being submitted. ***Do not*** staple payment to this inventory sheet or the fingerprint cards. Paper or binder clips are fine.
- ☐ ↑ **Mail this sheet, the corresponding applicant fingerprint card(s) and payment to the address shown under the Inventory Sheet Number above.** ***Do not*** separate this inventory sheet from the corresponding fingerprint cards and payment. The ***only*** materials that should be submitted to Applicant Team One are ***fingerprint card(s)***, ***inventory sheet(s)*** and ***payment***. ***Do not*** include additional paperwork with your submission unless otherwise instructed.

Distribution:
- White copy sent with fingerprint cards and payment to Applicant Team One.
- Canary copy for your files.

DPS 802-065013 Rev. 3-2011

Do not make copies of this inventory sheet for reuse, the inventory sheet number is unique to each sheet and cannot be duplicated.
Do not use this inventory sheet for criminal justice applicants.

2.10 Payment and Submission Packets

This subsection contains fee information and payment submittal requirements.

2.10.1 Fees

(Current fees as of August 2015)

Regular Applicant (state and FBI checks)	$22.00 per card
Applicants who are volunteers working with minors, 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 cashier's check, money order, or agency check to cover the total processing costs of the submitted fingerprint cards. (State agencies may also use state companion action transfers.) DPS DOES NOT accept personal checks, cash, or credit/debit cards.

Payment guidelines:

- Make the payment instrument payable to the **Department of Public Safety (DPS)**.
- 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 34 inventory sheets may be submitted in conjunction with any single payment instrument. If there are more than 34 inventory sheets full of names, please submit a separate check for those inventory sheet(s) in excess of 34 along with the associated fingerprint cards.
- The DPS Applicant Team cannot accept personal checks from applicants; direct deposit of applicants' personal checks to the DPS 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 DPS 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 of the following:

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

Send completed fingerprint packets to:

Arizona Department of Public Safety
Applicant Team – MD 2250
P.O. Box 18430
Phoenix, AZ 85005-8430

2.11 Rejected Fingerprint Cards/Resubmissions

When fingerprint submissions are rejected, you will receive a DPS 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 have to 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 which are rejected because the fingerprints are illegible or unclassifiable, a new fingerprint card will be needed. Follow the directions in your reject notice. Usually, you will need to complete a new inventory sheet and mark the "resubmit" box. Always include a copy of the reject notice with your resubmission; if you have an FBI reject sheet, be sure to send a copy of that with the resubmission as well.

Applicant cards rejected by the FBI for poor print quality can be resubmitted ONCE free of charge; however, the resubmitted card MUST be received by the FBI within one calendar year of the date of the original reject.

2.11.1 Name Searches on FBI Rejects

The FBI reject (ERRT) notice contains a reject code near the bottom of the page (see example). Currently, if the fingerprint reject sheet indicates code "L0008", the FBI has automatically already checked for criminal history using the applicant's name, date of birth, and social security number only. The applicant's name is not printed on the reject notice, only the fingerprint card's process control number.

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.
2.073: AZDPS2000

REASON FOR REJECT

There are two messages that may accompany a L0008 reject code:

- If the FBI results have a reject code L0008 and a message that reads *"The quality of characteristics is too low to be used"*, this means:
  - A name search was done with negative results.
  - **The submitting agency may elect to use these results as a negative name search or send in a new set of fingerprints for a second attempt at a fingerprint-based verification.**
  - The FBI reject notice does not state that a name search was done and it does not have the applicant's name printed on it. If the agency needs documentation that a name search was done, it must complete the routine name search procedure.

- If the FBI results contain the reject code L0008 and a message that reads *"The quality of 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)"*, this means:
  - There are possible results based on the name search.
  - **The agency will need to send in a new set of fingerprints AND the FBI ERRT (reject notice) response.**

2.11.2 Routine Name Search Procedure

If the agency is required to present a page with the applicant's name on it to prove negative FBI name search results, the agency must follow the routine name search procedure:

1) The fingerprints must have been rejected twice by the FBI.
   - The first reject must be within the past year.
   - The name search request must be submitted within 90 days following the second reject.

2) The agency must submit the CJIS Name Search Request Form. A copy of the instruction sheet (B-1) and the name search form (B-2) is in Appendix B of this guide. Fax or mail the request form to the DPS Applicant Team along with the applicant's two FBI reject notices.

2.12 DPS Results

The state results sent by DPS 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 DPS Results Report summary sheet similar to the one below; this page lists all the applicants that were contained on the inventory sheet sent by the agency and indicates results in the far right column.

EXAMPLE OF DPS RESULTS REPORT

FACTBDAP **Fingerprint Applicant Card Tracking System** **08/22/2014**
Agency Report of DPS ACJIS File Searches **Page 1**

(1) (2) (3)

Agency XX000000E NAME OF AGENCY **Sheet: 271300**

(4) **Date Received: 08/21/2014**

Applicant Name	DOB	Searched	DPS Results
Bear, Fuzzy D (5)	(6) **10/18/1982**	(7) **08/22/2014**	(8) **AZ00000311**
Kenobi, Ben	**09/23/1937**	**08/22/2014**	(9) *****
Skywalker, Luke	**01/01/1962**	**08/22/2014**	*****

*** = No record or no record meeting dissemination criteria**

LEGEND OF DPS RESULTS SHEET

(1) SUBMITTING AGENCY'S ORI

(2) SUBMITTING AGENCY'S NAME

(3) INVENTORY SHEET NUMBER

(4) DATE THE CARDS WERE RECEIVED AT AZ DPS

(5) APPLICANT'S NAME

(6) APPLICANT'S DATE OF BIRTH

(7) DATE THE STATE LEVEL SEARCH WAS CONDUCTED

(8) THE RESULTS OF THE STATE LEVEL SEARCH - "AZ" followed by eight numbers indicates a state identification (SID) number. A SID number indicates that applicant has a criminal history record.

(9) THE RESULTS OF THE STATE LEVEL SEARCH - An asterisk (*) indicates no record or no record meeting dissemination criteria was found.

NOTE:

One of the following may also appear in the DPS Results column:

"W" FOLLOWED BY A SERIES OF NUMBERS AND/OR LETTERS - INDICATES A WARRANT HIT.

"S" FOLLOWED BY 6 CHARACTERS - INDICATES THERE IS A SEX OFFENDER REGISTRATION RECORD.

EXAMPLE OF WARRANT

A.C.I.C. WANTED PERSON

(1)
BDG/ 3486 ORI/ AZACSPX00 OCA/ TEST0NLY1 DOW/ 01-14-2013 NOA/
AZ DPS,ACCESS INTEGRITY UNIT
(2) **NAM/ BEAR, TEST DOB/ 10-18-1983 SEX/ F RAC/ W POB/ CA**
HGT/ 502 WGT/ 115 EYE/ BLU HAI/ BLN SKN/ FAR SMT/

(3) **CRT/ MARICOPA COUNTY SUPERIOR CRT CTI/ BND/ NONE**
(4) **OFF/ AMPHETAMINE-POSSESS** (5) **(F) EXL/ STATE WIDE**
OOC/ WNO/ TEST1234567
ADR/ 2102 W ENCANTO BLVD, PHOENIX AZ DOP/
MIS/ CAUTION, MAY BE ARMED AND DANGEROUS
LSW WHI DRESS, WHI SHOES
THIS IS A TEST RECORD ONLY/NO VALID HIT/DO NOT ARREST

DTE/ 01-14-2013 TOE/ 12:59 DLU/ 01-14-2013 TOU/ 12:59 OPI/ 3487

CONFIRM WARRANT - EXTRADITION WITH ORI

NOTE: ***WARRANT INFORMATION IS NOT BASED ON FINGERPRINT COMPARISON; THEREFORE, THE DEPARTMENT CANNOT VERIFY THAT THE ATTACHED WARRANT DEFINITELY BELONGS TO THE ASSOCIATED APPLICANT.***

WANTED PERSON LEGEND

(1) DATE OF WARRANT (DOW)

(2) SUBJECT'S NAME

(3) AGENCY WHICH HOLDS THE ORIGINAL WARRANT

(4) OFFENSE (OFF)

(5) CLASSIFICATION OF CRIME
- (F) - Felony
- (M) - Misdemeanor
- (U) - Undesignated

EXAMPLE OF SEX OFFENDER RECORD

	DATE 08-22-2014 ARIZONA DEPARTMENT OF PUBLIC SAFETY PAGE 1 **TIME 07.51 SEX OFFENDER REGISTRATION INQUIRY RESPONSE** **INQUIRY RESPONSE BASED ON SOPN**
(1)	**SOPN/ 999997 NAM/ BEAR, FUZZY NIC/** **SID/ FBI/ 1111 INITIAL REG-DTE/ 08-05-2003** **CURRENT REG-ORI/ AZACSPX00 AZ DEPT PUB SFTY,ACCESS INTEG** **COMMUNITY NOTIFICATION REQUIRED/ NO PROFILE REC SOPN/**
(2)	**DOB/ 10/18/1982** **SEX/ M RAC/ U POB/AZ HGT/ 602 WGT/ 310 HAI/ BLK EYE/ BRO** **SMT/ ART L ARM SC FACE TAT R ARM** **SOC/ 123-45-6789** **AKA/ BEAR, REBEL FUZZY, DONLIKE** **RES ADDR AS OF 03-04-2012 PROP OWNER** **ADDR/ 12345 N NOPLACE STREET APT/ CITY/ PHOENIX** **CNTY/ MARICOPA ST/ AZ ZIP/ 85012 PHN/ 928-000-0000** **MAIL ADDR/** **OLS/ AZ OLN/ N9876543212 OLY/ 2001** **VLIS/ AZ VLIC/ TEST34 VLIT/ VLIY/** **VYR/ 1992 VMA/ OLDS VST/ VMO/ CAP VCO/ GRY**
	CONVICTION OFFENSE P TYP ARR/CNV DATE ARRESTING AGENCY/CONVICTION COURT (4) (5) (6)
(3)	**PUBLIC SEX INDECENCY M 05-06-2003 DPS** **08-04-2003 DPS COURT**
	EMP/ HOUSE OF HORRORS 999 EAST WITCH ROAD, SCAREY, AZ **PNT/ WICKED WITCH OF THE EAST 3321 N GOBLIN ST, SALEM, MA** **PROBATION OFFICER/RUFF MCGRUFF PHONE/** **CMT/ TEST RECORD NO VALID HIT** ***** DATA TO BE USED ONLY FOR CRIMINAL JUSTICE OR OTHER LAWFUL PURPOSES *****

LEGEND OF SEX OFFENDER RECORD

(1) SUBJECT'S SEX OFFENDER REGSTRATION NUMBER AND NAME

(2) SUBJECT'S DATE OF BIRTH

(3) OFFENSES(S)

(4) TYPE (Misdemeanor or Felony)

(5) ARREST & CONVICTION DATE(S)

(6) NAME OF ARRESTING AGENCY AND CONVICTING COURT

EXAMPLE OF ARIZONA CRIMINAL HISTORY RECORD

(1)
ACCH INQUIRY ON SID/AZ00000311
DATE 08-22-2014 ARIZONA DEPARTMENT OF PUBLIC SAFETY PAGE 0001
TIME 07.53 AUTOMATED CRIMINAL HISTORY
SID/ AZ00000311
THIS RECORD IS BEING RELEASED PURSUANT TO ARIZONA REVISED STATUTES, SECTION 41-1750. THIS INFORMATION MAY NOT BE FURTHER DISSEMINATED BY ANY MEDIUM, ORAL OR WRITTEN, TO ANY PERSON OR ENTITY UNLESS OTHERWISE AUTHORIZED BY LAW. ANY PERSON WHO KNOWINGLY OR RECKLESSLY PERMITS UNAUTHORIZED ACCESS OR RELEASES OR PROCURES THE RELEASE OF CRIMINAL HISTORY RECORD INFORMATION, OTHER THAN AS PROVIDED IN THIS SECTION, OR WHO USES SUCH INFORMATION FOR A PURPOSE OTHER THAN AS PROVIDED BY THIS SECTION IS GUILTY OF A CLASS 6 FELONY.
(2) (3)
NAM/ BEAR, FUZZY DE (4) **FBI/ SOC/ 123-45-6789**
SEX/ M RAC/ U DOB/ 10/18/1982 POB/ XX III STA/ DATE/
HGT/ 602 WGT/ 300 EYE/ BRO HAI/ BLK SKN/ PURGE ON/ 10-18-2081
HFP/ 16-M- 9- U-OOI-14 FPC/ 16-11-12-CI-14 DATE ENTERED 04-18-2001
M- 2- U-OOI- XX-XX-XX-XX-XX DATE UPDATED 01-14-2011
SMT/ ART L ARM SC FACE TAT R ARM PRCD EAR
RAP/ ** FELONY CONVICTIONS. (5)
AZ DOC NO./ 111111 CUSTODY STA/ 12-03-2003 EARNED CREDITS+TIME RELEASE
CUSTODY LOC/ ASPC-T SO AZ CORR REL CENTER
WARNING * * CUSTODY INFORMATION IS EXTRACTED FROM THE ARIZONA DEPT. OF CORRECTIONS AUTOMATED INMATE MANAGEMENT SYSTEM (AIMS) AND IS NOT BASED ON POSITIVE FINGERPRINT IDENTIFICATION.
COM/ TEST RECORD/ARTIFICIAL RESPIRATOR USED
ADDITIONAL IDENTIFIERS

DOB/ 10/18/1983 11/18/1982
SOC/ 013-65-8989 555-55-5555
AKA/ BEAR, FUZ FUZZY, DONLIKE BEAR, JES BEAR, REBEL
DATA TO BE USED ONLY FOR CRIMINAL JUSTICE OR OTHER LAWFUL PURPOSES.

***** (6)
ARREST/ 12-23-2000 AGENCY/ AZ0020000 COCHISE CO SO,BISBEE
NAME/ BEAR, FUZZY DE CASE/ R59883 PCN/
001 1006 KIDNAP-ADULT (7) (8) **FEL**
DISPO/ 10-02-2001 AGENCY/ AZ002015J COCHISE CO SUP CRT,BISBEE
1006 KIDNAP-ADULT FEL
(9) **DISPO/ GUILTY CASE/ C99TEST**
(10) **PRISON/ 1 YR OTH/ CONCURRENT**
002 1006 KIDNAP-ADULT FEL
DISPO/ 09-30-2001 AGENCY/ AZ002013J COCHISE CO SUP CRT, BISBEE
1006 KIDNAP-ADULT FEL
DISPO/ COURT DISMISSAL CASE/ C988TEST

003 1399 ASSAULT-INJ MIS * AMENDED
DISPO/ 09-30-2001 AGENCY/ AZ002013J COCHISE CO JUST CRT #1, BISBEE
1313 ASSAULT MIS
DISPO/ GUILTY CASE/ C988TEST
FINE/ 000250
OTH/ RESTITUTION 1000
004 1315 AGGRAV ASSLT-WPN FEL
DISPO/ 10-02-2001 AGENCY/ AZ002015J COCHISE CO SUP CRT,BISBEE
1315 AGGRAV ASSLT-WPN FEL
DISPO/ GUILTY CASE/ CR99TEST
PRISON/ 1 YR
OTH/ CONCURRENT

****
ARREST/ 01-29-2001 AGENCY/ AZ0070300 BUCKEYE PD
NAME/ BEAR, FUZZY DE CASE/ 323009 PCN/
001 4903 AIDING PRISONER ESCAPE FEL
DISPO/ 05-03-2001 AGENCY/ AZ007013A MARICOPA CO ATTY,INTAKE/LEJIS,PHOE
4903 AIDING PRISONER ESCAPE FEL
DISPO/ NO COMPLAINT FILED CASE/ CASE #UNK
002 1309 AGGRAV ASSLT-PUB OFF FEL * NEW CHG
DISPO/ 05-03-2001 AGENCY/ AZ007035J MARICOPA CO SUP CRT,PHOENIX
1309 AGGRAV ASSLT-PUB OFF FEL
DISPO/ GUILTY CASE/ C453TEST
PROBATION/ MARICOPA CO - 5 YEARS
OTH/ UNSUPERVISED

****
ARREST/ 05-06-2003 AGENCY/ AZCH7X000 AZ DEPT PUB SFTY,PHOENIX
NAME/ BEAR, REBEL CASE/ 523019 PCN/
001 4608 PUBLIC SEXUAL INDECENCY MIS
DISPO/ 08-04-2003 AGENCY/ AZ007WE0A WEIER JUS CRT, PHOENIX
4608 PUBLIC SEXUAL INDECENCY MIS
DISPO/ GUILTY CASE/ CASE NRC550
PROBATION/ MARICOPA CO - 3 YEARS
OTH/SUPERVISED, REG OFF

****
ARREST/ 03-08-2004 AGENCY/ AZ0090900 WINSLOW PD
NAME/ BEAR, FUZ CASE/ 876876 PCN/
001 0999 HOMICIDE FEL
(11) **DISPO/ NOT RECORDED**

****
ARREST/ 08-05-2005 AGENCY/ AZ0070000 MARICOPA CO SO,PHOENIX
NAME/ BEAR, FUZZY CASE/ 1234567890 PCN/
001 2299 BURGLARY FEL
DISPO/ 06-04-2006 AGENCY/ AZ007035J MARICOPA CO SUP CRT,PHOENIX
2299 BURGLARY FEL
(12) **DISPO/ CONVICTION VACATED CASE/ CR1234**
OTH/ PER ARS 13-907

****

ARREST/ 02-02-2008 AGENCY/ AZ0079953 AZ DEPT PUB SFTY,TEST ORI-530,ACJI
NAME/ BEAR, FUZZY CASE/ TEST PCN/
001 5001 BAIL-SECURED BOND MIS
DISPO/ 10-30-2009 AGENCY/ AZ007015G AZ BRD OF EXECUTIVE CLEMENCY
5001 BAIL-SECURED BOND MIS
DISPO/ CHARGES PARDONED/GOVERNOR CASE/ CR91TEST

****

ARREST/ 05-01-2008 AGENCY/ AZACSPX00 AZ DEPT PUB SFTY,ACCESS INTEGRITY
NAME/ FUZZY, DONLIKE CASE/ TEST PCN/
001 2499 STOLEN VEHICLE MIS
DISPO/ 05-01-2008 AGENCY/ AZACSPX00 AZ DEPT PUB SFTY,ACCESS INTEGRITY
2499 STOLEN VEHICLE MIS
DISPO/ NOT REFRD FOR PROSECUTION CASE/ CASE # UNK

****

ARREST/ 07-07-2012 AGENCY/ AZCCHPX00 AZ DEPT PUB SFTY,PHOENIX
NAME/ BEAR, JES CASE/ TEST PCN/ 9999999991
001 2404 VEH THEFT FEL
DISPO/ NOT RECORDED

DATA TO BE USED ONLY FOR CRIMINAL JUSTICE OR OTHER LAWFUL PURPOSES.

ARIZONA CRIMINAL HISTORY RECORD LEGEND

(1) SID - State Identification Number

(2) SUBJECT'S NAME

(3) SOCIAL SECURITY NUMBER

(4) DATE OF BIRTH

(5) RAP - This filled in gives an overview of the record. This example shows Department of Corrections prison information.

(6) DATE OF ARREST

(7) OFFENSE

(8) CATEGORY OF OFFENSE AT TIME OF ARREST (Felony or Misdemeanor)

(9) DISPO - Disposition of the case

(10) SENTENCING INFORMATION

(11) DISPO/ NOT RECORDED - This means the disposition of the case was not reported to the AZ Department of Public Safety.

(12) DISPO/ CONVICTION VACATED - Example of a court order entry. May also see court order information restoring a subject's civil rights, including the right to possess a firearm. In Arizona, the granting of a court order to vacate a judgment of guilt for a prior offense does not mean the arrest information is removed from the subject's criminal record. It only means that the vacate order will be appended to the file.

2.13 FBI Results

The FBI criminal history results will include a summary sheet similar to the example shown on this page. The results report page will contain all the applicants that were listed on a single inventory sheet.

EXAMPLE OF FBI RESULTS REPORT

```
FACTBMDP          Fingerprint Applicant Card Tracking System        06/01/2013
                 Report of FBI Results - Received on 05/31/2013
  Agency: XX000000E  EXAMPLE FBI RESULTS REPORT                Sheet: 123456

            (1)                          (2)          (3)          (4)        (5)
        Applicant Name                   PCN        From FBI      FBI       FBI
                                                      Date        Rslt     Number
------------------------------     ----------    ----------    ----    ---------
CLEEN, IBEE                        2A09123458    05/31/2013    N

WORNFINGERS, GLADYS                2A09123457    05/31/2013    P

XRAY, TEST                         2A09123456    05/31/2013    R       123456AZ7


                N = Negative, R = Hit, P = Rejected for Prints
```

LEGEND OF FBI RESULTS REPORT

(1) APPLICANT NAME

(2) PCN - Process Control Number. An applicant can be matched with both his/her fingerprint card and rap sheet or reject notice by using the PCN. The PCN is located toward the top of the FBI rap sheet/reject notice as well as on the barcode label of the fingerprint card.

(3) FROM FBI DATE - the date the FBI result was received by DPS for that applicant.

(4) FBI RSLT - FBI Results

- "R" - (which stands for Rap sheet) followed by an FBI number - criminal history was found. **An individual FBI rap sheet for EACH applicant should be enclosed.**
- "P" - the fingerprints were rejected by the FBI. **A SEPARATE reject notice should be enclosed.**
- "N" - negative result (no hit**). No additional paperwork is provided for the applicant.**

(5) FBI NUMBER - If the applicant has a criminal history, there will be a number in this column.

NOTE:

If FBI results are negative, the FBI Results Report will be the ONLY report the agency receives. No individual negative results will be provided.

If the applicant has a criminal history or the fingerprints are rejected, individual FBI rap sheets and print reject notices are included. If the fingerprint card was rejected and the agency is resubmitting the prints, be sure to include a copy of the actual reject notice from the FBI, *not* the FBI Results Report shown in the example above.

EXAMPLE INDIVIDUAL FBI REJECT NOTICE

```
     REJECT

     1.01:  158
     1.02:  0201
     1.03:  1
(1)  1.04:  ERRT
     1.05:  20021124
     1.06:  4
     1.07:  WVIAFIS0Z
     1.08:  WVIAFIS0Z
(2)  1.09:  IFCS000X151902662170
(3)  1.10:  2A09123457
     1.11:  00.00
     1.12:  00.00

     2.001: 466
     2.002: 00
(4)  2.006: XX000000E
     2.007:
(5)  2.060: L0008 – THE QUALITY OF THE CHARACTERISTICS IS TOO LOW TO BE USED.
(6)  2.073: AZDPS2000
     2.092:
     2.128:
     2.600:
```

FBI REJECT NOTICE LEGEND

(1) ERROR MESSAGE

(2) INFORMATION USED BY DPS FOR RESUBMISSION

(3) PCN NUMBER ASSIGNED BY DPS

(4) SUBMITTING AGENCIES ORI

(5) REJECT CODE AND REASON FOR REJECT

(6) DPS ORI

EXAMPLE OF FBI CRIMINAL HISTORY RECORD

IDENT RECORD (FBI RECORD)

1.1: 150
1.2: 0200
1.3: 1
1.4: SRE
1.5: 20021124 *
1.6: 4
1.7: WVIAFIS0Z
1.8: WVIAFIS0Z
(1) **1.9: IFCS000X151902662170**
(2) **1.10: 2A09123456**
1.11: 00.00
1.12: 00.00

2.1: 1113
2.2: 00
(3) **2.6: XX000000E**
(4) **2.18: XRAY, TEST**
(5) **2.59: I**
(6) **2.73: AZDPS2000**

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION
CLARKSBURG, WV 26306

AZDPS2000
PCN 2A09123456

THE FBI IDENTIFIED YOUR TEN-PRINT SUBMISSION WHICH CONTAINED THE FOLLOWING DESCRIPTORS:

(7) **NAME TEST, XRAY**
DATE ARRESTED/FINGERPRINTED 2013/04/28

(8)

SEX	RACE	BIRTH DATE	HEIGHT	WEIGHT	EYES	HAIR
MALE	WHITE	01/19/1954	603	235	BRO	BLK

STATE ID	BIRTH PLACE
	TEXAS

OTHER BIRTH DATES	SOCIAL SECURITY	MISC NUMBERS
NONE	XXX-XX-XXXX	NONE

ALIAS NAME(S)
NONE

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION
CLARKSBURG, WV 26306

BECAUSE ADDITIONS OR DELETIONS MAY BE MADE AT ANY TIME, A NEW COPY SHOULD BE REQUESTED WHEN NEEDED FOR SUBSEQUENT USE.

THIS RECORD IS SUBJECT TO THE FOLLOWING USE AND DISSEMINATION RESTRICTIONS

(9) **UNDER PROVISIONS SET FORTH IN TITLE 28, CODE OF FEDERAL REGULATIONS (CFR), SECTION 50.12, BOTH GOVERNMENTAL AND NONGOVERNMENTAL ENTITIES AUTHORIZED TO SUBMIT FINGERPRINTS AND RECEIVE FBI IDENTIFICATION RECORDS MUST NOTIFY THE INDIVIDUALS FINGERPRINTED THAT THE FINGERPRINTS WILL BE USED TO CHECK THE CRIMINAL HISTORY RECORDS OF THE FBI. IDENTIFICATION RECORDS OBTAINED FROM THE FBI MAY BE USED SOLELY FOR THE PURPOSE REQUESTED AND MAY NOT BE DISSEMINATED OUTSIDE THE RECEIVING DEPARTMENT, RELATED AGENCY OR OTHER AUTHORIZED ENTITY. IF THE INFORMATION ON THE RECORD IS USED TO DISQUALIFY AN APPLICANT, THE OFFICIAL MAKING DETERMINATION OF SUITABILITY FOR LICENSING OR EMPLOYMENT SHALL PROVIDE THE APPLICANT THE OPPORTUNITY TO COMPLETE, OR CHALLENGE THE ACCURACY OF, THE INFORMATION CONTAINED IN THE FBI IDENTIFICATION RECORD. THE DECIDING OFFICIAL SHOULD NOT DENY THE LICENSE OR EMPLOYMENT BASED ON THE INFORMATION IN THE RECORD UNTIL THE APPLICANT HAS BEEN AFFORDED A REASONABLE TIME TO CORRECT OR COMPLETE THE INFORMATION, OR HAS DECLINED TO DO SO. AN INDIVIDUAL SHOULD BE PRESUMED NOT GUILTY OF ANY CHARGE/ARREST FOR WHICH THERE IS NO FINAL DISPOSITION STATED ON THE RECORD OR OTHERWISE DETERMINED. IF THE APPLICANT WISHES TO CORRECT THE RECORD AS IT APPEARS IN THE FBI'S CJIS DIVISION RECORDS SYSTEM, THE APPLICANT SHOULD BE ADVISED THAT THE PROCEDURES TO CHANGE, CORRECT OR UPDATE THE RECORD ARE SET FORTH IN TITLE 28, CFR, SECTION 16.34.**

- FBI IDENTIFICATION RECORD -

WHEN EXPLANATION OF A CHARGE OR DISPOSITION IS NEEDED, COMMUNICATE DIRECTLY WITH THE AGENCY THAT FURNISHED THE DATA TO THE FBI.

NAME	FBI NO.	DATE REQUESTED
XRAY,TEST	123456AZ7	2013/05/30

SEX	RACE	BIRTH DATE	HEIGHT	WEIGHT	EYES	HAIR	BIRTH PLACE
M	W	1954/01/19	603	235	BRO	BLK	TEXAS

FINGERPRINT CLASS	PATTERN CLASS	CITZENSHIP
19 14 15 CO 16		UNITED STATES
16 PO 13 13 XX		

END OF PART 1 – PART 2 TO FOLLOW

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION
CLARKSBURG, WV 26306

AZDPS2000
PART 2

- FBI IDENTIFICATION RECORD - FBI NO. 123456AZ7

(10) **1-ARRESTED OR RECEIVED 1989/07/11**
AGENCY-SHERIFF'S OFFICE RIVERSIDE (CA0330000)
AGENCY CASE-20897
CHARGE 1-POSS NARC C/S

(11) **COURT-COUNTY COURT RIVERSIDE**
CHARGE-11350 HS-POSSESS NARCOTIC CONTROL SUBSTANCE
SENTENCE-
DIVERSION DISMISSED

(12) **2-ARRESTED OR RECEIVED 1995/02/13**
AGENCY-POLICE DEPARTMENT FRESNO (CA0100500)
AGENCY CASE-8502137001
CHARGE 1-DRIVING WITH LICENSE INVALID

3-ARRESTED OR RECEIVED 2005/05/26
AGENCY-POLICE DEPARTMENT CEDAR PARK (TX2460900)
AGENCY CASE-56302
CHARGE-AGG ASSAULT SBI

COURT-26th DISTRICT COURT GEORGETOWN (TX246015J)
CHARGE-AGG ASSAULT CAUSES SERIOUS BODILY INJURY
SENTENCE-
2006-04-23 DEFERRED PRB-5Y0M0D FNE-2500

4-ARRESTED OR RECEIVED 2011/09/03
AGENCY-SHERIFF'S OFFICE GEORGETOWN (TX2460000)
AGENCY CASE-11586
CHARGE-THEFT >$20 <$500 BY CHECK

COURT-COUNTY COURT GEORGETOWN (TX246013J)
CHARGE-THEFT CLASS C MISDEMEANOR
SENTENCE-
2011-12-01 CONVICTED LESSER CHARGE FNE-0200

ALL ARREST ENTRIES CONTAINED IN THIS FBI RECORD ARE BASED ON FINGERPRINT COMPARISONS AND PERTAIN TO THE SAME INDIVIDUAL.

THE USE OF THIS RECORD IS REGULATED BY LAW. IT IS PROVIDED FOR OFFICIAL USE ONLY AND MAY BE USED ONLY FOR THE PURPOSE REQUESTED.

FEDERAL CRIMINAL HISTORY RECORD LEGEND

(1) INFORMATION USED BY DPS FOR RESUBMISSION

(2) PCN NUMBER ASSIGNED BY DPS

(3) ORI OF SUBMITTING AGENCY

(4) SUBJECTS NAME

(5) IDENT (MEANS FBI RECORD)

(6) DPS ORI

(7) SUBJECT'S NAME

(8) SUBJECT'S PERSONAL IDENTIFIERS

(9) FEDERAL USE AND DISSEMINATION RESTRICTIONS

(10) ARREST INFORMATION
- DATE ARRESTED OR DATE FINGERPRINT CARD RECEIVED BY FBI

(11) COURT INFORMATION
- SENTENCE (LOOK FOR DISPOSITION HERE FOR ABOVE ARREST)

(12) ARREST INFORMATION (SECOND ARREST - DIFFERENT DATE AND AGENCY)
- NO COURT AND NO DISPOSITION NOTED IN EXAMPLE

Section 3 - Basic Privacy and 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.

- Access:
  - Defining who is authorized to access CJI/CHRI
  - Restricting access to only those who are authorized
- Use:
  - Defining the 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 discuss the criminal record contents with the applicant within the confines of the purpose for which it was given:

- 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 in order to ascertain if the circumstances of the issue warrant denial.
- The agency MAY NOT give 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)

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** give 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 own 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 **www.fbi.gov** under *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 to 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 device (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 which 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 give CJI/CHRI to any other agency or individual unless specifically authorized by law. This is called "secondary dissemination".

Secondary dissemination can only occur to an authorized recipient. All secondary dissemination must be logged, and the log shall be retained for five years. The log should clearly 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 complete 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 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 prior to 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 completely 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) prior to complete 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 to 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 which 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 are aware of the consequences that may result from unauthorized use of CJI/CHRI.

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

- Give 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 cancelled 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 theft of public records for personal gain and Title 18 USC §1030 which discusses unauthorized access to protected information via computer.

Unauthorized release could potentially expose the organization and/or individual to civil liability.

In addition, 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 DPS and is responsible for coordinating agency compliance with all federal and state laws/regulations pertaining to 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 DPS for all communication regarding audits, training, and security. The ASC is also the first point of contact for DPS in the event of an allegation of criminal history misuse or a security issue involving the criminal history check process. It is important that the ASC's contact information stay updated with the DPS Access Integrity Unit in order to allow for 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 online at *www.azdps.gov* under NCJA Fingerprint Compliance. Forms may be emailed, faxed, or mailed to the Access Integrity Unit. (See the Contact List on page 4.)

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 D for a copy of this form or the DPS website under NCJA Compliance.)
- For the agency's convenience, this form asks if the agency is also appointing the new ASC as the Applicant Team contact. <u>If this box on the form is checked</u>, then the Noncriminal Justice Compliance Team will update the contact with the Applicant Team as well.
- 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 D or go online to the DPS website for the form.) 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.

- DPS will send out 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 D or go online to the DPS website for the form.)
- The Noncriminal Justice Compliance Team will acknowledge receipt of the form and update the information with the DPS Applicant Team, if applicable. If further information is required, a Noncriminal Justice Compliance Specialist will contact the ASC with any questions.

4.1.2 Authorized Personnel List

The ASC must submit an Authorized Personnel List to the AIU Noncriminal Justice Compliance Team. The Authorized Personnel List contains all agency personnel who are authorized to receive, view, handle, disseminate, store, retrieve, or dispose of CJI/CHRI. The Authorized Personnel List 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 give 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 Authorized Personnel List can be found in Appendix C of this guide and also online on the DPS website under Noncriminal Justice Compliance. The <u>entire</u> Authorized Personnel List 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). Mark new additions with an asterisk or other indicator. (Make sure the ASC is on the Authorized Personnel List!) The agency should retain one copy of the Authorized Personnel List for its records and forward a copy to the AIU Noncriminal Justice Compliance Team.

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 within six months of hire or being 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 from the DPS website under Noncriminal Justice Compliance.

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 on the consequences of misuse of CJI/CHRI; training must be repeated every two years. 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 DPS for training**. DPS's compliance training is designed to help the Agency Security Contact or other designated agency representative understand the new compliance requirements so that they can implement the rules back at their agency; DPS 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 Noncriminal Justice Compliance Team upon request. A blank Training Documentation Form is located in Appendix E of this guide and is also available for download from the DPS website under NCJA Fingerprint Compliance.

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.

The ASC is responsible for entering the date Acknowledgement Statements were signed on the Training Documentation form. Do not send the acknowledgement statements to DPS; 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 in a timely manner.
- 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 which submit fingerprints for criminal history checks are subject to audit to ensure that they are in 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 in order to assess compliance with state and federal policies and regulations. DPS Access Integrity Unit (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 Unit 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 prior to 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 assessment questionnaires and charts 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 triggered 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 DPS:

- Receives a complaint from an agency or individual alleging misuse of CJI/CHRI.
- Becomes aware of agency actions which 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 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 period of time, DPS will contact the ASC’s supervisor, agency CEO, or other administrator.

The review by an AIU Compliance Specialist is designed to detect process issues which may result in noncompliant actions by an agency. Areas which will be audited are the same ones that are checked during a routine audit; in addition, 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 in order to bring the agency into compliance so that it can continue to utilize the fingerprint criminal history check process through DPS. 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 which require correction, an agency may be scheduled for a routine audit after a specified period of time in order 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 DPS that allows DPS to provide CJI/CHRI upon 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 DPS. The Authorized Personnel List 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 - don't 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 DPS 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 DPS.
   The Compliance Specialist will look for procedures which establish either a process which 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 to 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 PRIOR to 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 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 28 CFR 16.34.

Additionally:

- The agency should also establish and document what constitutes a reasonable period of 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 security and dissemination of CJI/CHRI. Section 3 of this guide covers required policies and basic privacy and security guidelines.

1) The agency must have a process which 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 a 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 DPS 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 every two years. 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 an outline of 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 NCJA Training Documentation Form (or equivalent) and the documentation must be available for inspection by auditors.

Section 6 - DPS Classes & Assistance

DPS provides free training to noncriminal justice agencies receiving criminal justice information and criminal history record information. DPS's compliance training is designed to help the Agency Security Contact or other designated agency representative understand the new compliance requirements so that they can implement the rules back at their agency; DPS 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. **Authorized Personnel DO NOT need to come to DPS for training**.

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 F of this guide or online in the Noncriminal Justice Compliance section of the DPS website. The current training calendar is also available online. **There are no fees for these classes**.

6.1 Initial Access Training

All new agencies are required to have at least one representative attend Initial Access Training prior to submitting any fingerprint cards. Initial Access 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 in order 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.

Class Description

Initial Access 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/criminal history record information
- Overview of basic privacy and security guidelines
- Brief overview of agency/ASC requirements and responsibilities

Recommended for: Personnel responsible for the agency's fingerprint submission process
Agency Security Contact (ASC)

6.2 NCJA Compliance Training

In addition to the Initial Access Training, the DPS Access Integrity Unit offers training classes to assist user agencies with complying with state and federal requirements associated with noncriminal justice fingerprint criminal history checks. NCJA Compliance Training is not a required training class; however, it is highly recommended for new agencies and for existing agencies which are unfamiliar with the Arizona Noncriminal Justice Compliance Program. New agencies should complete Initial Access Training before attending NCJA Compliance.

Class Description

NCJA Compliance Training lasts approximately three hours and outlines the Agency Security Contact's role as the primary user agency liaison and provides guidance regarding user agency regulatory compliance and required documentation. Basic privacy and security guidelines for the access, use, handling, and destruction of criminal history record information are discussed as well as key areas for agencies to consider when developing policies/procedures for criminal history handling. Authorized Personnel training requirements and

an overview of CJIS Online Security Awareness training are also covered. This training is for the Agency Security Contact and agency trainers – this is NOT the training which is required for agency Authorized Personnel. Authorized Personnel training requirements are explained in the class.

Recommended for: Agency Security Contact, Agency trainers

6.3 Additional Training Offered by DPS

The DPS Access Integrity Unit may offer other classes from time to time to address specific agency concerns or attempt to address demand for a special type of refresher training. All current classes will appear on the training schedule and will be announced in the monthly 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".

6.4 Obtaining Assistance from DPS

Please note that there are different DPS 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 Access Integrity Unit 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 & NCJA 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 card and inventory sheet supplies

The DPS 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/ArizonaRevisedStatutes.asp

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

Arizona Administrative Code Title 13: www.azsos.gov/public_services/

Federal References

United States Code of Federal Regulations: http://ecfr.gpoaccess.gov

- 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 USC 552 Freedom of Information Act
- Title 5 USC 552a Privacy Act of 1974 (as amended)
- Title 42 USC 14616 Compact Council

Federal Bureau of Investigation: 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 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 pertaining to 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.
ARS	Arizona Revised Statutes	The Arizona laws enacted by the State Legislature. The most updated version can be found online at www.azleg.state.az.us/ArizonaRevisedStatutes.asp
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 that is the main receiving point through which agencies in the state access systems managed by the FBI CJIS Division. The CSA in Arizona is the Department of Public Safety.
CSO	CJIS Systems Officer	Person from the CSA who is responsible in ensuring the state's users are in compliance 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 DPS headquarters in Phoenix.
DPS	Arizona Department of Public Safety	State level law enforcement agency protecting the property and citizens of Arizona. DPS also operates the Arizona Central State Repository.
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	Federal level network that houses various databases on persons and property.
NCJA	Noncriminal Justice Agency	For the purposes of 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 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.

ORDERING ***APPLICANT TEAM*** SUPPLIES

PLEASE COMPLETE THIS FORM AND FAX OR MAIL TO:

Arizona Department of Public Safety
Applicant Team
Mail Drop 2250
P.O. Box 18430
Phoenix, AZ 85005-8430

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

ITEM	**AMOUNT REQUESTED**
Applicant Fingerprint Cards	_____
Inventory Forms (802-06513) (If you pay a fee for services)	_____

Agency Name: _____

Agency ORI: _____

Address: _____

_____

_____

Telephone #: _____

Order Date: _____

PLEASE ALLOW 2-3 WEEKS FOR PROCESSING OF ORDER

ARIZONA DEPARTMENT
OF PUBLIC SAFETY
Mail Drop 2250
P.O. BOX 18430
Phoenix, Arizona 85005-8430

Telephone: **(602) 223-2722**
FAX: **(602) 223-2972**

FROM: **Arizona Department of Public Safety**
Applicant Team

REMARKS:

The attached form is to request the FBI to complete a name, date of birth, and social security number check on an applicant that has been rejected twice by the FBI. The PCN is the number on the bar code. Put in the PCN numbers of the last 2 cards that were rejected by the FBI. Write your agency's ORI in the OCA field. When completed, FAX the form to the Applicant Team. It takes 2 to 3 weeks to get the results back from the FBI depending on their volume. The results will be forwarded to your agency.

- **The first reject must be within the past year.**
- **The second reject must be within 90 days of the name search request.**

If the FBI cannot process the request they will fax it back with a reject notice that will indicate why.

Make copies of the form for future use.

CJIS NAME SEARCH REQUEST FORM

Please complete the attached form to request a name check. A name check 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: CHRISTOPHER RAMSEY

Phone number of POC: (602) 223-2722

Fax number of POC: (602) 223-2972

Address of requesting agency: APPLICANT TEAM
PO BOX 18430
MD 2250
PHOENIX, AZ 85005-8430

Please fax my response to this request.

Subject of Name Check

Transaction Control Number (PCN) of subject's fingerprint submission: 2A18_____

2A18_____

Name: _____ Alias: _____

Date of Birth: _____ Place of Birth: _____

Sex: _____ Race: _____ Height: _____ Weight: _____ Eyes: _____ Hair: _____

Social Security Number: _____

OCA: XX_____

***Please note that bolded fields are required for name check searches.**

Requesting agency _____

Date faxed to DPS _____

(DPS use only)
DATE TO FBI_____

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 Dept of Public Safety
Access Integrity Unit – M/D 1190
Noncriminal Justice Compliance Team
P.O. Box 6638
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**
Lu, Lorax	Boss
Farry, Trie	2nd Boss
Squirrel, Sarah *	Admin Asst
Bear, Smart (ASC)	Director
Inthamiddle, Skunk	Receptionist

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

Sincerely,

Smart Bear
Agency Security Contact
Human Resources Director, Earth Traditional Academy

EXAMPLE

Arizona Department of Public Safety

Noncriminal Justice Agency *Information Change* Form

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

Change ASC (To designate this person as the Applicant Team contact as well, mark this box. ☐)	***Previous* ASC Name**		
	New ASC Information		
	Title	**Name**	
	New ASC Contact Information		
If changing ASC Contact Info only, Mark this box. ☐)	**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: (If you wish to designate a secondary ASC, please use this box.)	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 - MD 1190
ATTN: Noncriminal Justice Compliance
P.O. Box 6638
Phoenix, AZ 85005-6638

OR

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

Email: NCJA@azdps.gov

NONCRIMINAL JUSTICE AGENCY TRAINING DOCUMENTATION FORM

AGENCY NAME: _____ ORI/OCA: _____

The following training is REQUIRED:

Security Awareness Training (CJIS Online)

This training must be completed within 6 months of hire or appointment to position with access to criminal justice/criminal history record information. It 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.

Agency Internal Privacy and Security Training

Any personnel placed on the agency authorized Personnel List should receive 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. Refresher training shall be completed every two years.

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 or online in the NCJA Fingerprint Compliance section of the DPS website. Updated training schedules and special classes are also periodically posted online. Classes are free of charge.

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

Training Reservation Form

Agency Name	**Date**
ASC Name	**ASC Phone**
ASC Email	

	CLASS NAME	**Date Requested**	**# of Attendees**
_____	**Initial Access Training (REQUIRED for new Agencies)**	_____	_____
_____	**NCJA Compliance Training**	_____	_____
_____	**Compliance Refresher Training**	_____	_____
_____	**Other: _____**	_____	_____

Send completed form to:

Arizona Department of Public Safety
Access Integrity Unit - MD 1190
ATTN: Noncriminal Justice Compliance
P.O. Box 6638
Phoenix, AZ 85005-6638

OR

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

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

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 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** **_____**	