Introduction

In January 2013, the Arizona Noncriminal Justice Compliance Program went into effect. This program was formulated in response to FBI CJIS Division rules requiring routine compliance audits for agencies which use criminal history record information (CHRI) for noncriminal justice purposes such as employment and licensing. Compliance audits are conducted by the DPS Access Integrity Unit. The Noncriminal Justice Compliance Program has an informational website: Go the www.azdps.gov, look under Services, then select Governmental Services then click on NCJ.

Compliance Overview

The routine audits associated with the Arizona Noncriminal Justice Compliance Program evaluate agency adherence to federal and state laws as well as FBI regulations and National Crime Prevention and Privacy Compact Council guidelines. The following is a summary of the compliance areas reviewed during a routine noncriminal justice audit.

1. Agency Security Contact (ASC)
   Each agency must appoint an ASC. The ASC is the main contact for the agency for noncriminal justice CHRI compliance purposes.

2. Authorized Personnel List
   Each agency must submit an Authorized Personnel List to the DPS Access Integrity Unit. All personnel who view, handle, use, discuss, disseminate, or dispose of criminal history must appear on the list. An example Authorized Personnel List can be downloaded from the NCJ Compliance website.

3. Required Training
   A. Privacy & Security Training
      All Authorized Personnel must undergo two-part privacy and security training at your agency.

      1) Part 1 - CJIS Online Training
         The link for the training site is located in the CJIS Online section of the NCJ Compliance webpage. Be sure to download the CJIS Online Training Supplement – this contains the log-in for the training and essential information for those taking the training. CJIS Online training must be completed within 6 months of hire/appointment to the Authorized Personnel List and repeated every two years.

      2) Part 2 - Agency-specific privacy and security processes
         You must identify/create your agency's policies/procedures for handling CHRI. Once you have determined that you have the required internal policies/procedures, you must document that you have trained your personnel on those policies/procedures. This training must be repeated every two years.

B. Acknowledgement Statements

All Authorized Personnel need to sign an Acknowledgement Statement created by the agency. There is no standard format for the statement; however, the statement must say at a minimum that the individual acknowledges notification of the consequences for misuse of criminal history.

C. Training Documentation

All required privacy and security training must be documented on the Training Documentation Form. The Training Documentation Form is available on the NCJ Compliance website.

4. Quality Assurance

Due to concerns raised regarding another person posing as an applicant when being fingerprinted and the potential for an applicant to tamper with the information on a previously verified fingerprint card, agencies should establish and document processes used for fingerprinting quality assurance. The National Crime Prevention and Privacy Compact Council's *Identity Verification Program Guide* offers suggestions for quality assurance measures.

A. Quality assurance methods to verify applicant identity

Ideally, applicants are identified using valid, unexpired photo identification. Agencies that allow/require applicants to be fingerprinted at locations other than on-site can use instruction sheets and chain-of-custody forms to assist the fingerprinting entities with proper identification in order to ensure quality results.

B. Quality assurance methods to safeguard the integrity of fingerprints prior to processing

Agencies should employ methods to prevent tampering with the fingerprint card prior to its processing. This could include methods that require mailing the fingerprint card directly to the agency or employing a "sealed envelope" or other system to prevent the applicant's direct access to the completed card. This may include establishing procedures for rejection of "open" prints that are hand-carried by applicants or mailed in from the applicant unsealed.

5. Policies and procedures

Agencies must have policies/procedures that cover the following points. If there are existing agency/department processes that adequately cover these issues, these must be identified and incorporated into the required training (#2 under privacy & security training).

A. Processes which provide the required privacy rights notifications to applicants (28 CFR 50.12b)

Agencies must advise the person being fingerprinted of the following notifications PRIOR to submitting the fingerprint card to the FBI (via DPS). The DPS *Guidelines for Required FBI Notifications of Applicant Privacy Rights* summarizes this requirement.

1) 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 must be provided in a format where applicants can read and take a copy with them if they desire.

2) All applicants must be informed that they are allowed a reasonable opportunity to complete and challenge the accuracy of the criminal history record. Agencies need to establish processes for what constitutes a "reasonable opportunity" and for appeals.

3) 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.

B. Policies/procedures for access, use, handling, dissemination, and destruction of CHRI

At a minimum, these policies/procedures must cover how the applicable basic privacy & security guidelines are incorporated into the agency's processes. Basic privacy & security guidelines are outlined in Section 3 of the NCJ Agency Guide. These policies/procedures can be a combination of agency/bureau policies and agency administrative procedures. These policies/procedures should include provisions for:

1) Ensuring that CHRI is used only for the purpose for which it is requested
2) Preventing unauthorized access to CHRI
3) Maintaining CHRI in a secure manner
4) Proper retention/destruction of CHRI
5) Secondary dissemination (if applicable)
6) Technical compliance (if CHRI is accessed/stored electronically)
7) Formal disciplinary process for misuse

Assistance

Please contact the DPS Access Integrity Unit Noncriminal Justice Compliance Team with any questions you have regarding the compliance program.

Noncriminal Justice Compliance Team email:
NCJA@azdps.gov

Phone: (602) 223-2488

Noncriminal Justice Compliance website:
http://www.azdps.gov/services/government/ncj