Idaho State Police

NCJA CRIMINAL HISTORY RECORD INFORMATION(CHRI) GUIDELINES

Non-Criminal Justice Agency User Training Manual and Self-Inspection Checklist

gwalker
01/15/2013

Idaho State Police

Service since 1939

Bureau of Criminal Identification

Criminal History Record Information (CHRI)

(Guidelines for qualified "Authorized Recipients" receiving applicant CHRI)

AUTHORITIES FOR RECEIVING CHRI

- Title 5, United States Code (U.S.C.), Section 552, the Freedom of Information Act.
- Title 28, U.S.C., § 534, authorizes dissemination of CHRI, and provides that access to CHRI is subject to cancellation if dissemination is made outside of the authorized recipient.
- Title 5, U.S.C., § 552a, the Privacy Act, requires that agencies maintain a system of records which establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records.
- Title 42, U.S.C., Chapter 140, Subchapter II, § 14616, the Compact, established the Compact Council, which is authorized to establish rules, procedures, and standards for the use of Interstate Identification Index (III) for non-criminal justice purposes. Determining compliance includes, but is not limited to: assessing participation requirements; the continual maintenance; and security of CHRI.
- Title 28, Code of Federal Regulations (CFR), 20.30, cites the administration of criminal justice shall include criminal identification activities, and the collection, storage and dissemination of CHRI.
- Title 28, CFR, 20.33 (a) (2), authorizes the dissemination of CHRI contained in the III to federal agencies authorized to receive it pursuant to federal statute or Executive Order.
- Title 28, CFR, 20.33 (a) (3), authorizes the dissemination of CHRI contained in the III for use in connection with licensing or employment, pursuant to Public Law (Pub. L.) 92-544, 86 Stat. 1115, or other federal legislation, and for other uses for which dissemination is authorized by federal law.
- Title 28, CFR, 50.12 (b), references the exchange of FBI identification records obtained

under this authority may be used solely for the purpose requested and cannot be disseminated outside the receiving departments, related agencies, or other authorized entities.

- Title 28, CFR, § 0.85 (j), The Director of the Federal Bureau of Investigation shall: (a) Investigate violations of the laws … In investigating violations of such laws and in collecting evidence in such cases, the Director may exercise so much of the authority vested in the Attorney General by sections 1 and 2 of Reorganization Plan No. 1 of 1968, section 1 of Reorganization Plan No… (j) Exercise the power and authority vested in the Attorney General to approve and conduct the exchanges of identification records enumerated at 50.12(a) of this chapter.

- Title 28, CFR, Part 906, Outsourcing of Non-criminal Justice Administrative Functions, amends the dissemination restrictions of 28 CFR 50.12 (b) by permitting the outsourcing of non-criminal justice criminal history record checks to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency.

- Title 28, CFR, Part 906, the Outsourcing Standard, requires contractors to maintain a security program consistent with federal and state laws, regulations, and standards, as well as, with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

CHRI GENERAL ACCESS/USE INFORMATION

Criminal History Record Information (CHRI) must be maintained in locked file cabinets and must NOT be accessible to any persons not authorized to access criminal history/privacy information.

Access to applicant CHRI shall comply with the National Crime Prevention and Privacy Compact, the Federal Bureau of Investigation (FBI)/Criminal Justice Information System (CJIS) Security Policy. This security policy provides guidelines for state and local agencies whose authority to receive CHRI has been identified, promulgated (to include the specific language required by law) and approved by the proper authority under one or more of the following options:

- City Ordinance
- State Statute
- Public Law 92-544
- The National Child Protection Act (NCPA)
- The Volunteers for Children Act (VCA)

Agencies subject to Public Law 92-544 for accessing CHRI from the FBI for purposes of licensing and employment must have enacted a state statute or city ordinance that has been approved by the Attorney General of the United States, whose approval authority has been delegated to the FBI by Title 28, CFR § 0.85(j). The standards employed by the FBI in

approving Pub. L. 92-544 purposes have been established by a series of memoranda issued by the Department of Justice (DOJ), Office of the General Counsel (OGC), Access Integrity Unit (AIU). The standards are:

- The authorization must exist as the result of legislative enactment or its functional equivalent;
- The authorization must require fingerprinting of the applicant;
- The authorization must, expressly or by implication, authorize use of FBI records for screening of the applicant;
- The authorization must not be against public policy;
- The authorization must not be overly broad in its scope; it must identify the specific category of applicants/licensees.

Additionally,

- The fingerprint submission must be channeled through the State Bureau of Criminal Identification (BCI) for forwarding to the FBI;
- The states must designate a governmental agency to be responsible for receiving and screening the results of the record check to determine an applicant's suitability for employment/licensing;
- The results of the record check cannot be released outside the receiving governmental department or related governmental agency;
- Processing fees are either by direct payment or billed to the State BCI depending on arrangements made between the FBI and the BCI, such as the execution of a Memorandum of Understanding for billing.

When changes to an approved state statute occur, the statute must be re-submitted to the AIU for approval. (Compact Council Topic Paper 8/08, Topic #1, Attachment #1, pg. 4)

A Non-Criminal Justice Agency (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for non-criminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy. (CJIS Security Policy 5.1; 5.1.1.6)

The agency must create formal written procedures which "apply to the handling, processing, storing and communication of criminal justice information…no matter the form of exchange." (CJIS Security Policy 5.1; 5.1.1.1)

Frequency of Fingerprint-based Records Requests

Pursuant to Idaho Code § 67-3012 Article IV(c)(2) which requires "that subsequent record checks are requested to obtain current information whenever a new need arises", NCJA's

receiving federal authorization to access CHRI must determine that frequency dependant on the needs of the agency and incorporate that frequency in the agency's formal written policies.

The National Child Protection Act of 1993, as amended, permits qualified entities to receive state and federal criminal history information to assist in the screening of employees and volunteers who provide care, treatment, education, training, instruction, supervision or recreation to children, older adults or individuals with disabilities. The mission of the NCPA program is to protect:

- Children (any unmarried person under 18 years of age, who has not been emancipated by order to the court);
- Older Adults (a person who is 60 years of age or older);
- Individuals with disabilities (persons with a mental or physical impairment who require assistance to perform one or more daily living tasks)

Agencies wanting to become a "qualified entity" under the ISP NCPA program (*see page 14 of this document for NCPA specific self inspection questions*) for access to federal and state CHRI, must complete an application and user agreement to be approved by the BCI Manager. The user agency must agree to:

- Submit requests to ISP for criminal history background checks only for current or prospective Idaho employees and volunteers for whom the agency is not already required to obtain state and national criminal history checks under any other state or federal statutory provision;
- Determine whether the current or prospective employee or volunteer has been convicted of, or is under pending indictment for, a crime that bears upon his or her fitness to have access to or contact with children, the elderly, or individuals with disabilities;
- Obtain a completed and signed Waiver Agreement and Statement form (provided by ISP) from every current or prospective employee and volunteer, for whom the agency submits a request for a criminal history background check to ISP. This waiver must be kept on file at the agency for as long as the employee or volunteer is working for the agency, or for five years, whichever is longer;
- Use only fingerprint cards provided by ISP specifically designed for use with requests for criminal history record checks under the NCPA; provide ISP with a properly completed and executed fingerprint card for each current or prospective employee and volunteer for whom User requests a criminal history record check; and indicate either :NCPA/VCA Volunteer" or "NCPA/VCA Employee" in the "reason fingerprinted" block of each fingerprint card submitted;
- Keep all records necessary to facilitate a security audit by ISP and to cooperate in such audits as ISP or other authorities may deem necessary. Records that may be subject to

audit are criminal history records; notification that an individual has no criminal history; internal policies and procedures articulating the provisions for physical security; records of all disseminations of criminal history information; and a current, executed User Agreement with ISP;

- Keep criminal history records separate from other records, whether such other records are public or not;
- Duplication and/or dissemination of criminal history records is prohibited for use outside of the authorized recipient agency, except as authorized by state and federal law;
- Current computerized criminal history must be requested and relied upon if criminal activity is pertinent to and considered at the time of an employee or volunteer's service;
- Ensure that the appropriate personnel know to keep the information obtained from the fingerprint based background check requests in a secure place and to use it only for the screening as outlined in the User Agreement;
- Promptly advise ISP of any violations of the User Agreement.(NCPA User Agreement)

Proper Use of CHRI

CHRI may only be used for an authorized purpose, consistent with the purpose for which it was requested. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including—but not limited to—employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances. (CJIS Security Policy 5.1, 4.2.2.1/5.1.1.1)

Penalties

CJIS systems data (including CHRI) is sensitive information and security shall be afforded to prevent any unauthorized access, use, or dissemination of the information. Improper access, use and/or dissemination of CHRI is serious and may result in the imposition of administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

The Idaho State Police Bureau of Criminal Identification accepts electronic civil fingerprint card submissions from agencies authorized to submit fingerprint cards for criminal history nationwide checks. Agencies meeting specific requirements may receive Hit/Non Hit confirmations via emails. This email does not include any detailed CHRI. A hard copy of any hit (criminal history record) will be sent to the agency via US Postal first class mail. It is the responsibility of the agency to maintain and update contact information with BCI. Future capabilities for electronic distribution of CHRI will be disseminated as the technologies are developed. If your agency would like to begin submitting fingerprints electronically, please contact: Maria Wiley, BCI Applicant Unit Supervisor, 208-884-7159 or maria.wiley@isp.idaho.gov.

Self Inspection Questions for Access/Use (all NCJAs)

1. **List the specific authority(s) under which your agency receives CHRI. (e.g., IdC 18-3302)**
2. **Has the authority(s) under which your agency requests state and federal criminal history record information been enacted by the state or local jurisdiction and approved by the FBI?**
3. **Does your agency have formal written policies and procedures regarding access to and use of CHRI?**
4. **List all categories of applicants included in the authority under which your agency requests and receives CHRI.**
5. **Does your agency limit the personnel authorized to receive and view CHRI? List all positions and job titles of personnel in your agency who are designated to use/access CHRI.**
6. **List all names and job titles of the personnel assigned to make the employment/licensing fitness determinations for your agency.**
7. **Does your agency use CHRI only for the purpose for which it was requested?**

CHRI PRIVACY AND SECURITY INFORMATION

The CJIS Security Policy does not authorize access to CHRI to maintenance personnel, contractors, custodians or any other employee or potential employee not authorized to handle CHRI and they shall be escorted entry while in the area where CHRI is maintained.

CHRI ***cannot be*** handled by a third party entity not involved in making the fitness determination on the applicant. Any positions or boards designated to view CHRI must be specified in detail in the Agency's statute authorizing National Criminal History checks on their classification of applicants.

Criminal Justice Information (CJI) Security

The computer site and related infrastructures (e.g., information system servers, controlled interface equipment, associated peripherals, communications equipment, wire closets, patch panels, etc., if they house equipment which provides access to the CJIS network) must have adequate physical security at all times to protect against any unauthorized access to or routine

viewing of computer devices, access devices, and printed and stored data. (CJIS Security Policy 4.5, 4.4.1)

A physically secure location is a facility or an area, a room or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Those perimeters shall be defined, controlled and secured in a manner acceptable to ISP BCI. The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel. The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access. (CJIS Security Policy 5.1, 5.9.1)

If an agency cannot meet all the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a "controlled area" for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum:

- Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI;
- Lock the area, room, or storage container when unattended;
- Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view;
- Follow the encryption requirements found in section 5.10.1.1.2 of the CJIS Security Policy, for electronic storage (i.e. data "at rest") of CJI. (CJIS Security Policy 5.1, 5.9.2)

If an agency wants to receive CHRI via electronic means, there are a number of technical requirements to control how the data moves from one place to the next in a secure manner. For more information on the technical requirements, please contact Gary Walker, ISP Applicant Auditor/Trainer at gary.walker@isp.idaho.gov or Matt Mennear, ISP Information Systems Officer at matt.mennear@isp.idaho.gov.

Personnel Security

At a minimum, the following topics shall be addressed as **Baseline Security Awareness Training** for all authorized personnel with access to CJI:

- Rules that describe responsibilities and expected behavior with regard to CJI usage.
- Implications of noncompliance.
- Incident response (Points of contact; Individual actions).
- Media protection.

- Visitor control and physical access to spaces—discuss applicable physical security policy and procedures (e.g., challenge strangers, report unusual activity).
- Protect information subject to confidentiality concerns—hardcopy through destruction.
- Proper handling and marking of CJI.
- Threats, vulnerabilities, and risks associated with handling of CJI.
- Dissemination and destruction. (CJIS Security Policy 5.1, 5.2.1.1)

Baseline Security Awareness Training is the responsibility of the agency. All non-criminal justice agencies will be responsible for creating and implementing a training program for employees based on the CHRI usage of the agency. By 2013, all non-criminal justice agencies must institute a Security Awareness Training program; they must keep a current list of authorized employees who are allowed access to CHRI; and be able to show that the employee received the awareness training. There will also be an ISP Security Awareness Training module that authorized personnel will complete and records of that training will be maintained at the agency.

Currently there is not a requirement for employees of a *non-criminal justice agency*, which receives CHRI, to be subject to a CHRI check if not statutorily authorized. Although there is not a requirement, the CJIS Division Advisory Policy Board and the Compact Council recommend as a best business practice for non-criminal justice agency that employees be subject to the CHRI check, prior to having access to CHRI. (Compact Council Topic Paper 8/08, Topic #1, Attachment #1, pg. 14)

Self Inspection Questions for Security (all NCJAs)

1. **Is CHRI kept in a physically secure location? Describe in detail.**
2. **How is access to the secure location restricted to authorized personnel only?**
3. **Have all personnel who have been authorized to access CHRI been trained in security measures with regards to the safeguarding of CJI?**
4. **Does your agency have a current and complete list of all personnel authorized to handle CHRI?**
5. **Has your agency created a formal security awareness training program for all personnel with access to CHRI?**
6. **Does your agency conduct any personnel screening prior to access to CHRI? If yes, describe in detail.**

CHRI STORAGE/RETENTION AND DISSEMINATION INFORMATION

Storage/Retention

CHRI records shall be stored in a secure records environment. When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files. For agencies housing records electronically, please contact the Bureau of Criminal Identification, Audit and Training section at gary.walker@isp.idaho.gov. (CJIS Security Policy 5.1, 4.2.4)

Dissemination

CHRI cannot be shared with any internal or external body not involved in the fitness determination of an applicant, outlined in the Authorized recipient's statutory authority. CHRI can be given to the applicant upon request or in-person where the applicant's identity can be verified. The delivery of CHRI to the applicant can be mailed USPS mail, after a waiver has been signed by the applicant requesting a copy.

Authority to disseminate or share CHRI shall be approved by the Idaho State Compact Council Officer and Bureau of Criminal Identification Manager. The request to disseminate CHRI must be concurrent with the Compact Council, *Outsourcing Standard* established by the Privacy Compact Council and CJIS Security Policy. A written agreement must be accomplished between the authorized recipient of CHRI and the prospective contractor with whom the authorized recipient is requesting to share CHRI.

Penalties for unauthorized disclosures

Title 28, U.S.C., § 534, Pub. L. 92-544 and Title 28, CFR, 20.33(b), provide that the exchange of records and information is subject to CANCELLATION if dissemination is made outside the receiving departments or related agencies. Furthermore, depending upon the nature of the offense and the identity of the offender, federal or state crimes may be charged for the willful, unauthorized disclosure of CHRI. Penalties may be different depending on the authority to which the CHRI was authorized for dissemination.

Self Inspection Questions for Storage/Retention and Dissemination (all NCJAs)

1. **How long does your agency retain CHRI?**
2. **Does your agency have formal written policies and procedures for the storage, retention and dissemination of CHRI?**
3. **Does your agency maintain CHRI in an electronic format/database?**
4. **Is the database, password protected, standalone, etc.?**
5. **Does your agency disseminate CHRI outside of the receiving agency? If yes, for what purpose?**
6. **Is CHRI given to the applicant? If yes, describe the process.**

CHRI DESTRUCTION AND OUTSOURCING INFORMATION

Destruction

Destruction of CHRI shall be conducted only by authorized recipients approved under one of the recognized authorities listed above and shall be pursuant to the Privacy Compact Council's Outsourcing standard and the CJIS security policy.

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel. (CJIS Security Policy 5.1, 5.8.4)

Electronic media shall be sanitized, that is, overwritten at least three times or degaussed prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitation or destruction is witnessed or carried out by authorized personnel. (CJIS Security Policy 5.1, 5.8.3)

Outsourcing

Outsourcing of any non-criminal justice agency functions involved with an authorized recipient's authority to receive CHRI is **not authorized**, unless approved by the State Compact Council Officer. This policy is applicable to the following operations:

- Fingerprinting

- Use of CHRI
- Access to CHRI files
- Physical security of electronic/hard copy CHRI and hit/non hit notifications
- Retention of CHRI
- Destruction
- Dissemination

The goal of the Compact Council Security and Management Control Outsourcing Standard is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of the Outsourcing Standard is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security. The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule.

Contractors authorized to perform non-criminal justice administrative functions requiring access to CHRI without a direct connection to the FBI's CJIS WAN must adhere to all applicable provisions of this Outsourcing Standard. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform non-criminal justice administrative functions requiring access to CHRI without a direct connection to the FBI CJIS Wide Area Network (WAN). (National Crime Prevention and Privacy Compact Council, Security and Management Control Outsourcing Standard; 5/10, pg. 1)

Non-criminal Justice Administrative Functions means the routine non-criminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:

1. Making fitness determinations/recommendations;
2. Obtaining missing dispositions;
3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General;
4. Other authorized activities relating to the general handling, use, and storage of CHRI.

The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the terms of the contract. (Compact Council Outsourcing Standard; 5/10, 1.09; 2.05)

If an agency would like to outsource any administrative function involving CHRI received from BCI, a written request must be submitted to the Idaho State Police Bureau of Criminal Identification.

Self Inspection Questions for Destruction and Outsourcing (all NCJAs)

1. **Does your agency have formal written policies and procedures for destruction of CHRI?**
2. **Does your agency policy for destruction of CHRI include a stipulation that an authorized agency employee witness or carry out the destruction?**
3. **Does your agency outsource any non-criminal justice administrative functions to a Contractor?**
4. **Did your agency, as the Authorized Recipient, request and receive written permission from the State Compact Officer/Chief Administrator of the Repository to outsource CHRI?**
5. **Is the Contractor given direct access to CHRI?**
6. **What administrative function is the Contractor providing to the authorized recipient?**
7. **Does the Contractor have a security program?**
8. **Does the Authorized Recipient agency have policies and procedures in place to monitor and/or audit the security processes of the Contractor?**
9. **Are Contractor personnel handling CHRI required to undergo the same level of screening that the Authorized Recipient personnel with access to CHRI?**

NCPA Specific Self Inspection Questions

1. **Does your agency submit fingerprint-based background check requests for those current or prospective employees/volunteers for whom the agency is not already required to obtain state and national criminal history background checks under any other state or federal statutory provision?**
2. **Does your agency determine whether the current or prospective employee/volunteer has been convicted of, or is under pending indictment for, a crime that bears upon his or her fitness to have access to or contact with children, the elderly or individuals with disabilities?**
3. **Does your agency retain the original signed and dated waiver agreement and statement for all personnel for whom a fingerprint-based criminal history records request was made for the length of employee/volunteer service or five (5) years, whichever is longer?**
4. **Is the correct reason for fingerprinting, "NCPA/VCA Employee" or "NCPA/VCA Volunteer" indicated properly on each fingerprint card submitted to ISP? Does your agency include the agency's assigned identifying NCPA number on each fingerprint card submission as instructed by BCI?**
5. **Does your agency co-mingle criminal history records with other records, whether such other records are public or not?**
6. **Does your agency duplicate and/or disseminate criminal history records for use outside the User entity?**
7. **Does your agency require a current criminal history records check for consideration at the time of an employee or volunteer's service?**
8. **Does your agency store criminal history records in a secure file, safe, or other security device, such as locked file cabinet in an access-controlled area; also taking such further steps as are necessary to ensure that the records are accessible only to those of its employees who have been trained in their proper use and handling and who have a need to examine such records?**

BEST PRACTICES

The demand for fingerprint-based background checks for non-criminal justice purposes has increased significantly over the past few years. If the agency has implemented FBI guidelines for best business practices, they will not require corrective actions, unless the procedures have a clear violation of regulation, statute, policies, or law. Please contact the Bureau of Criminal Identification, Audit and Training section at gary.walker@isp.idaho.gov with questions or comments. (Compact Council Topic Paper 8/08, Topic #1, Attachment #1, pg. 14)

Training

Basic Security Awareness training is required (2013 audit cycle) for all authorized personnel of non-criminal justice agencies with access to CJI as per the *CJIS Security Policy*. In addition, the Compact Council encourages that any Qualified Entity, fingerprinting applicants for licensing/employment purposes, train employees in taking legible fingerprints. This best business practice will increase the likelihood of receiving accurate criminal history information and decrease agency liability regarding licensing/employment decisions. The FBI's training manual for Taking Legible Fingerprints is attached to this document as Appendix A.

Chain of Custody

Fingerprinting agencies and contractors have expressed concern that applicants with a criminal history record may have someone pose as the applicant for fingerprinting purposes. Therefore, the Compact Council prepared the *Identity Verification Program Guide* in response to these concerns. This guide is for voluntary use in the development of policy, procedures, and practices for applicant identity verification. It also includes a listing of primary and secondary identification, data support documents, and chain of custody procedures. An agency may employ a process to protect the integrity of the fingerprints when they are forwarded to the SIB and/or the FBI. Proper chain-of-custody procedures increase the possibility of an accurate record search. The *Identity Verification Program Guide* is attached to this document and can also be requested electronically from the ISP Audit and Training section. (Compact Council Topic Paper 8/08, Topic #1, Attachment #1, pg. 14)

Privacy Notification and Subsequent Uses of Non-criminal Justice Fingerprint Submissions

Currently, the IAFIS Civil File contains more than 26 million records of persons fingerprinted for employment, licensing, security assessments, or other non-criminal justice purposes. Such purposes include authorized federal background check programs and military service; persons fingerprinted for visa, alien registration, immigration, naturalization, or related Department of State or DHS security purposes; persons desiring to have their fingerprints placed on record with the FBI for personal identification purposes; and individuals fingerprinted for authorized national security purposes. In accordance with the Privacy Act of 1974 and the E-Government Act of 2002, the FBI has provided public notice of the categories of records that it maintains within the

Fingerprint identification Records System. *The FBI **does not retain** non-criminal justice fingerprint submissions for those applying for license or employment governed by Public Law (Pub.L.) 92-544.*

It is the responsibility of the agency collecting the fingerprints (and associated descriptive data) to inform the person being fingerprinted of the authority to collect the information and its potential use. Civil fingerprint submissions are often collected manually on FBI applicant cards (FD-258) or via electronic fingerprint capturing devices. This information is then provided to authorized agencies in support of federal criminal history checks. Those persons being fingerprinted on the FD-258 fingerprint cards are required to provide a signature for verification and authorization purposes at the time of fingerprinting. If an agency uses a livescan device to capture fingerprints for noncriminal justice purposes, the CJIS Division staff recommends that the agency should implement an electronic signature capability or provide a copy of the back of the FD-258 for the applicant to sign which would indicate that the applicant understands the potential use of the submission.

In addition, officials making the determination of suitability for licensing and employment purposes "shall provide the applicant the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record." These officials must also advise the applicant of the procedures for obtaining a change, correction, or update to an FBI identification record as set forth in Title 28, Code of Federal Regulations, (C.F.R.) Section 16.34. A statement incorporating the use and challenge requirements is required to be placed on records disseminated for these purposes. (CJIS Information Letter, 12/6/10)

To obtain a copy of the statement that appears on the FBI's rapsheets in response to non-criminal justice employment/licensing fingerprint submissions, please contact Gary Walker, BCI Applicant Auditor/Trainer at gary.walker@isp.idaho.gov.

AUDITING

Audit programs are designed to determine compliance with applicable system rules, regulations, policies, and guidelines.

Non-criminal Justice Agency Audits

The BCI Audit Unit shall conduct a compliance audit triennially of each authorized recipient with statutory authority to receive CHRI in order to verify compliance with applicable statutes, regulations and policies. Compliance audits may be conducted on a more frequent basis if the audit reveals that an agency has not met the compliance standards. (CJIS Security Policy 5.1, 5.11.2)

The purpose of the audit is to assess compliance with non-criminal justice use and the appropriate rules pertaining to the security, maintenance, and dissemination of CHRI. Idaho Non-criminal Justice Agencies will be on a 3year audit cycle. The first audit is an informational audit for the purpose of educating nontraditional users and should be used to establish proper procedures and policies for the access, use, and dissemination of CHRI. Subsequent audits are cycle one, two, etc. (Compact Council Topic Paper 8/08, Topic #1, Attachment #1, pg. 7)

Audit Methodology

Approximately, one month prior to the audit, the ISP BCI Auditor will contact the agency announcing the audit either by phone, email, or letter. The Auditor will explain the audit process, required timelines and the scope of the audit. The agency will be provided with a Pre-audit Self Inspection Checklist along with the state CHRI Guidelines and a Pre-Audit Questionnaire, if these documents have not been provided previously. The auditor will confirm agency Point of Contact (POC) information and set a mutually agreeable audit date with the POC.

During the interval between contact and the audit, the BCI auditor will review data samples from the agency based on:

- Statutory Authority Review
- ORI to RFP comparison/usage
- Fingerprint rejection rate/Live scan process review
- Pre-audit questionnaire regarding agency policies and procedures regarding the access, use, storage, retention, dissemination, destruction and general handling of CHRI

Results of the review will be discussed at the audit. Depending on time and budget constraints, the NCJA audit may be conducted on-site, by mail or by phone. During the audit, auditors may conduct on-site administrative interviews with appropriate representatives for the selected agencies. Interviews may also be conducted with entities to which the State Identification Bureau (SIB)/State Repository and selected agencies have outsourced third-party support services for non-criminal justice administrative functions. The interview may include a contract/agreement review, and when applicable, a physical security review of CHRI. If your agency is audited through a mail-in audit, you will have up to 4 weeks to complete it and a telephone interview may be conducted with the Point of Contact (POC) to verify your agency's answers to the audit questionnaire, if necessary.

When the audit has been completed, the BCI Auditor will have 10 business days to finalize the audit report for supervisory review, addressing noncompliance issues for corrective action and recommendations for presentation to the Agency Head. Upon receipt of the audit report, agencies will have 30 days to review the report and respond to any discrepancies. If corrective actions are required, the agency will respond with its proposed action plan and the Auditor will process the proposals and re-audit or respond to the agency.

**For questions regarding Non-criminal Justice Agency (NCJA) auditing please contact Gary Walker at gary.walker@isp.idaho.gov. **

UNDERSTANDING CRIMINAL HISTORY REPORTS

What is a Criminal History Record Report - also known as a "rap" sheet?

A "rap" (**R**ecord of **A**rrest and **P**rosecution) sheet is a record of arrest and convictions anywhere in Idaho for a person 17 years or older. Rap sheets are maintained by the Idaho State Police, Bureau of Criminal Identification. Each time a person is arrested and fingerprinted, the booking agency sends a report of the arrest to the Bureau. A rap sheet contains information only for Idaho, but the Federal Bureau of Investigation (FBI) is notified of all arrests across the country. A rap sheet can be viewed by almost anyone who specifically requests a copy from the State of Idaho by following the requesting guidelines found in the Idaho State Police website, under the Bureau of Criminal Identification, Applicant Background Checks.

What is expungement?

Expungement is a court filing that erases arrests and convictions from the record.

What can be expunged?

Idaho Code 67-3004(10) states the following:

Any person who was arrested or served a criminal summons and who subsequently was not charged by indictment or information within one (1) year of the arrest or summons and any person who was acquitted of all offenses arising from an arrest or criminal summons may have the fingerprint and criminal history record taken in connection with the incident expunged pursuant to the person's written request directed to the department.

What is a conviction?

A conviction occurs when a person pleads guilty to a crime or is found guilty by a judge or jury after a trial. A guilty plea also includes conditional discharge for any time served. Conviction information is considered public information in Idaho.

What is a felony?

A felony under Federal law is a crime that is punishable by a prison sentence of more than one year. Under Idaho state law, a felony is any crime that can be punished by death or by imprisonment in a state prison.

What is a misdemeanor?

A misdemeanor is less serious than a felony. Except in cases where a different punishment is prescribed, every offense declared to be a misdemeanor, is punishable by imprisonment in a county jail not exceeding six (6) months, or by a fine not exceeding one thousand dollars ($1,000), or by both.

What is probation?

Probation is a sentence in which conditional freedom is granted after a conviction or a guilty plea, with requirements for certain behaviors by the offender. When an offender violates any agreement/behavior while on probation, he/she may have their probation revoked and be required to serve out the rest of their time in a correctional facility.

What is parole?

Parole is the conditional release of a prison inmate after serving part (if not all) of his or her sentence, allowing the inmate to live in the community under supervision of the parole period. The decision to grant parole is the responsibility, in a majority of states, of a commission or board of parole. Violation of the conditions of parole results in revocation and re-imprisonment.

What is provided regarding Arrests?

1-Arrest Date: Date arrested

2-ORI: FBI assigned number identifying the arresting agency

3-Agency: Agency that completed the fingerprinting as a result of the arrest

4-Case: Case number assigned by the arresting agency

5-Charge: (M) misdemeanor or (F) felony charge – literal explanation of the arrest

6-Counts: Lists number of counts charged against the individual at the time of arrest

What does disposition mean?

The disposition on a criminal record is the final outcome, or resolution, of a court case or criminal matter.

What is provided regarding Dispositions?

7-Court: Once the issue goes to court, a number identifier is assigned to the record

8-Charge: (M) misdemeanor or (F) felony charge – literal explanation of the disposition of the charge - based on the courts judgment. Often, this is a reduction of the original arrest.

9-Counts: Lists number of counts charged against the individual at the time of arrest

10-Disp/Sent: This will be the court's conclusion of the sentence involving the arrest. If available, this will contain dismissal information, sentencing information, fine/court cost information, restitution information, probation information, and numerous other detailed items. Also included will be dates, if provided by the court's conclusion.

IDENTITY VERIFICATION PROGRAM GUIDE FOR FINGERPRINTING

(PREPARED BY THE NATIONAL CRIME PREVENTION AND PRIVACY COMPACT COUNCIL)

The National Crime Prevention and Privacy Compact Council (Compact Council) is a 15 member body of local, state, and federal governmental officials which prescribes system rules and procedures for the effective and proper operation of the Interstate Identification Index (III) for non-criminal justice purposes.

In recent years, the demand for fingerprint based background checks for non-criminal justice purposes has increased. Fingerprinting agencies and contractors alike have expressed concern that applicants with a criminal history record may have someone pose as the applicant for fingerprinting purposes. In response to these concerns, the Compact Council prepared this guide for voluntary use in the development of policy, procedures, and practices for applicant identity verification.

FACTORS TO CONSIDER

(For the purpose of this guide, "agency" will refer to any agency or contractor responsible for the capture and/or submission of fingerprints for non-criminal justice purposes.)

In the course of establishing an applicant verification program, agencies may choose to consider the following factors:

- ✓ Clearly define and document policy, procedure, and practices. Document what is accomplished and how it is performed.
- ✓ Review current business policy, procedures and practices regarding verification, training, legal obligations, and privacy implications that may be incorporated into a program.
- ✓ Develop an understanding of the use of various biometric-based systems.

Since the state repository manages the processing of fingerprint submissions to the FBI, it is suggested that appropriate coordination and liaison be established at that level as a preliminary step toward an applicant identity verification program.

FINGERPRINTER CERTIFICATION

Another preliminary consideration for states may be the enacting of a Public Law 92-544 based statute establishing a certification process that qualifies the employees capturing the applicant's fingerprints. This may include a requirement for a fingerprint-based background check of those employees.

In developing a fingerprint application verification program, the Compact Council suggests establishing written policy, procedures, and practices. The following guide may be helpful in the process.

- ✓ Determine Policy, Procedures, and Practices
- ✓ Create an Identification Validation Guide
- ✓ Create Chain of Custody Procedures

Policy, Procedures, and Practices may include:

A. Training in the capture of fingerprints (rolled or flats, and electronic or manual)

B. Certification of employees performing duties under the scope of the identity verification program, which may include recognizing and validating authorized identification forms, identification documents, and source documents for identity confirmation

C. Security considerations:

- ✓ Train employees to recognize and handle the various identification form security features such as biometric features and machine-readable technology.
- ✓ Assign a unique identification number to each employee to be included with each fingerprint submission.
- ✓ Train employees to recognize official identification forms, documents, and fraudulent or counterfeit documents.

PRIMARY AND SECONDARY IDENTIFICATION

Currently most agencies request some type of photo identification card as one method for verifying an individual's identity. The compact Council suggests agencies accept only current, valid, and unexpired picture identification documents. As a primary form of picture identification, a state-issued driver's license* which meets the requirements of Public Law 109-13 may be presented by an applicant when being fingerprinted. However, in the absence of the new driver's license, applicants may provide one or more secondary documents including:

- ✓ State Government Issued Certificate of Birth
- ✓ U.S. Active Duty/Retiree/Reservist Military Identification Card (000 10-2)
- ✓ U.S. Passport
- ✓ Federal Government Personal Identity Verification Card (PIV)
- ✓ Department of Defense Common Access Card
- ✓ U.S. Tribal or Bureau of Indian Affairs Identification Card

- ✓ Social Security Card
- ✓ Court Order for Name Change/Gender Change/Adoption/Divorce
- ✓ Marriage Certificate (Government Certificate Issued)
- ✓ U.S. Government Issued Consular Report of Birth Abroad
- ✓ Foreign Passport with Appropriate Immigration Document(s)
- ✓ Certificate of Citizenship (N560)
- ✓ Certificate of Naturalization (N550)
- ✓ INS I-551 Resident Alien Card Issued Since 1997
- ✓ INS I-668 Temporary Resident Identification Card
- ✓ INS I-688B, I-766 Employment Authorization Card

** For those applicants without a driver's license, a state identification card may be presented if the state's identification card standards are the same as for the driver's license.**

DATA SUPPORT COVERAGE

When validating the authenticity of secondary identification documents and forms, the data and information may be supported by at least two of the following:

- ✓ Utility Bill (Address)
- ✓ Jurisdictional Voter Registration Card
- ✓ Vehicle Registration Card/Title
- ✓ Paycheck Stub with Name/Address
- ✓ Jurisdictional Public Assistance Card
- ✓ Spouse/Parent Affidavit
- ✓ Cancelled Check or Bank Statement
- ✓ Mortgage Documents

DATA SUPPORT METHODS

When supplemental documentation does not support the validation of the original identification documents, the agency may choose any or all of the following methods to validate the authenticity of the documents:

- ✓ Physically examines the applicant's photograph on the identification form/card.
- ✓ Visually compare the picture with the applicant in person.
- ✓ Compare the physical descriptors of the applicant to the documentation provided by the applicant. (I.e. height, weight, hair and eye color, age, etc.)
- ✓ Request the applicant to verbally provide date of birth, address, etc. and check this against the identification forms used.
- ✓ Check the applicant's signature in person with that on the identification form.
- ✓ Ensure that the identification form has not been altered in any manner.

- ✓ If available, verify that the machine readable data matches the data on the card when it is scanned.

When an agency has a reason to believe an applicant has presented fraudulent information, agency personnel should contact local law enforcement. No attempt should be made to detain or pursue the person.

CHAIN OF CUSTODY PROCEDURES

An agency may employ a process to protect the integrity of the applicant's fingerprints when they are forwarded to the state identification bureau and/or the FBI.

The following information provides a guide to developing a chain of custody process:

A. Establish provisions for the agency to manage both manually and electronically captured fingerprints.

B. Establish an agency tracking system (applicant log) using the employee's name or some other method for identifying the individual capturing the fingerprints and verifying the applicant's identity.

C. Establish procedure that documents the type of identification used by the applicant.

D. Establish procedures that use specially sealed envelopes, agency specific stamps, etc. for the agency to use when forwarding the applicant's manually captured fingerprints.

E. Implement the use of form(s), which may include the:

1. Date of fingerprinting
2. Reason for fingerprinting
3. Printed name, signature, and/or identification number of the employee taking the fingerprints
4. Name of employee's supervisor
5. Supervisor's signature
6. Address of agency to receive fingerprints
7. Name of agency and physical address where fingerprinting was performed
8. Type of fingerprint capture (rolled ink, flat ink, live scan, etc.)
9. Applicant's disclosure information