



Next Generation Identification Audit

Noncriminal Justice Access to Criminal History Record Information

Policy Reference Guide



Telephone – 304-625-3020
E-mail – <NISAudit@leo.gov>

Table of Contents

Criminal History Record Information	1
Use of CHRI	2
Fingerprint-based	
Coordination and Approval	
Authorized Requests	
Implementation	
Re-use	
Name-based	
Coordination and Approval	
Authorized Requests	
Implementation	
Re-use	
Dissemination of CHRI	5
Authorized Recipients	
Receiving Departments	
Related Agencies	
Single Need/Purpose	
Multiple Needs/Purposes	
Other Authorized Entities	
Jurisdictional Control	
Public Access	
Additional Considerations	
General	
Notifications	
Subject of the Record	
Residual Access	
Purpose for Disclosure of CHRI	11
Reason Fingerprinted Field	
Interstate Identification Index Purpose Codes	
Reason for Request	
Agency Identifiers for Receipt of CHRI	
Independent Application, Fingerprinting, and Adjudication Processes	
Documentation of Reason for Request	
Applicant Notification	12
FBI Privacy Act Statement	
FBI Record Access and Amendment	
Additional Considerations	
Noncriminal Justice Agency Audits	17
User Fee	17
Criminal Justice (No-fee)	
Volunteer (Reduced-fee)	
Abbreviations and Acronyms	19

Criminal History Record Information

The Compact, at Title 34, U.S.C., Section 40316, Article I, includes the same statutory definition of CHRI as that established at Title 28, CFR, Section 20.3: information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release; the term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system. In addition, the *CJIS Security Policy* defines CHRI as a subset of Criminal Justice Information consisting of any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information, or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Information is considered CHRI if it is transferred or reproduced directly from CHRI received as a result of a national FBI check and associated with the subject of the record. This includes information such as conviction/disposition data as well as identifiers used to index records regardless of format. Examples of formal and informal products or verbalizations include: correspondence such as letters and e-mails; documents such as forms and hand-written notes; conversations either in person or by telephone; and data fields such as those stored in database tables or spreadsheets. However, information is not considered CHRI if it is obtained as a result of using CHRI received from a national FBI check as a lead to reach out to source record owners such as local courts or state criminal history record repositories. As a prerequisite, both the process used to obtain the source record information and the resulting source record information itself must not directly reference or be attributed to the national FBI check.

Information is considered CHRI if it confirms the existence or nonexistence of CHRI. This FBI policy is derived from and mirrors the general policy on dissemination found at Title 28, CFR, Section 20.21, directly relating to applicable state and local criminal history record information systems. This includes applicant status information, which is either directly attributed to or predominately based on a national FBI check, when no recognized authority or inherent need exists for the release of such information.

Use of CHRI

The requirements for the use of CHRI for noncriminal justice purposes are derived from various federal statutes, regulations, policies, and interpretations thereof, to include rules and procedures promulgated by the Compact Council. Primary references for these requirements include:

- Title 28, U.S.C., Section 534 (a)(4)
- Title 34, U.S.C., Section 40316, Article IV (c) and Article V (a) and (c)
- Title 28, CFR, Section 20.33
- Title 28, CFR, Section 50.12
- Title 28, CFR, Section 901
- *III/NFF Operational and Technical Manual*, Chapter 3
- CJIS Advisory Policy Board, *Concept for the Exchange of Criminal History Records for Noncriminal Justice Uses by Means of The III*, Section B
- Compact Council's Noncriminal Justice Online Policy Resources

The NGI audit assesses four categories of requirements associated with the use of CHRI for noncriminal justice purposes: (1) Authorized Requests, (2) Implementation, and (3) Re-use. While baseline requirements for both fingerprint-based and name-based use of CHRI for noncriminal justice purposes essentially parallel one another, the four categories of requirements are presented from both perspectives for clarity and reporting purposes.

Use of CHRI (Fingerprint-based)

Unless authorized pursuant to federal statutory authority or Compact Council regulations promulgated based upon federal statutory authority, noncriminal justice background checks of the III System must be supported by fingerprints or other approved forms of positive identification in order to determine that the subject of a record search is the same person as the subject of a criminal history record indexed in the III System. This requirement is memorialized in the Compact. The Compact Council has accepted two methods for determining positive identification for exchanging CHRI for noncriminal justice purposes, ten-rolled fingerprints and ten-flat fingerprints.

Coordination and Approval

Agencies must only leverage recognized/approved authorities for submission of noncriminal justice fingerprint-based requests for CHRI. Examples of such authorities include Public Law 92-544, the NCPA/VCA, the Adam Walsh Act, and the Serve America Act. Prior to implementation of any federal statutory authority, a state or federal agency must coordinate with the FBI to determine the requirements for submitting under the specific authority (e.g., system changes, issuance of an ORI, fingerprint submission procedures, use of specific reason fingerprinted, etc.), and when applicable, obtain formal approval prior to use. When applicable, agencies must also obtain updated approval from the FBI for any changes associated with a previously approved authority, such as Public Law 92-544 state statutes. In addition, agencies must notify the FBI which authority is the exclusive remedy when multiple approved authorities exist for a particular purpose (applicant type). This specific requirement currently applies when states must formally designate either an approved Public Law 92-544 state statute or the NCPA/VCA for providers of care to vulnerable populations if state law is not clear or silent on the NCPA/VCA.

Authorized Requests

Agencies must only submit noncriminal justice fingerprint-based requests for CHRI for purposes (applicant types) covered by the authority leveraged for the request. In addition, agencies must only submit requests for purposes that are known to exist at the time of submission. Agencies must not submit requests for a future anticipated need, even if the need is covered by an approved authority.

Implementation

Agencies must implement all applicable administrative and procedural provisions associated with the authority leveraged to submit noncriminal justice fingerprint-based requests for CHRI (e.g., signed applicant statements under NCPA/VCA and VECHS agency user agreements).

Re-use

Agencies must only use CHRI received as a result of noncriminal justice fingerprint-based requests for the specific purpose originally requested. Agencies must not subsequently re-use CHRI for unrelated needs, even if the new needs are covered by a recognized/approved authority. A purpose or need for use is a request for CHRI to adjudicate a specific application for a noncriminal justice purpose (e.g., license, position of employment, benefit, etc.) that is known at the time the request is made, pursuant to an approved statutory authority, and based on the positive identification via fingerprint submission of the applicant. The basic parameters for use consists of (chronologically): 1) authority for access, 2) application and fingerprint submission, 3) receipt of CHRI, 4) adjudication, and 5) closing or maintenance activities.

However, if a special set of circumstances exist that show an extremely close relation to the original purpose, CHRI that was made available for the original purpose could possibly be used again for the new purpose. Under this premise, the new purpose is so closely related to the original purpose that both are considered singular in nature. The primary factors when considering the circumstances that may potentially relate multiple purposes include: the statutory authority being used; the agency or agencies involved; the type of license/position of employment/benefit being applied for; and the application/adjudication process. This consideration is based on standing audit practices and legal interpretations of related agency as applied to the use of CHRI. It is important to note that this type of acceptable re-use is quite infrequent and very dependent upon the specific scenario involved. As such, it is highly recommended that re-use of this nature be closely coordinated with the FBI prior to implementation. For example, a person applies to be a substitute teacher with public School Board A. School Board A completes the fingerprint process and submits the fingerprints pursuant to an approved state statute that authorizes background checks for school employment purposes. Then one month later the individual also applies to be a substitute teacher with public School Board B. School Board B requests a copy of the CHRI from School Board A which provides it. In this case, since School Board A and School Board B are both covered by the same statute and using CHRI for a similar applicant type within a relatively short period of time, these can be considered to be for the same purpose. However, if the applicant had applied one month later for a liquor license from the ABC Board, School Board A would not be permitted to provide the CHRI to the ABC Board. Although the background checks are in a relatively short period of time of each other, the applicant types are significantly

different enough, and the ABC Board would not be covered by the same statutory authority as School Board A. In addition, CHRI may be re-used in limited circumstances under the NCPA/VCA VECHS program.

It is important to note that FBI CHRI is considered instantly outdated as new information may be added to the record or deleted at any time. Although re-use of CHRI in certain situations may be acceptable, agencies that accept the risk of using outdated CHRI must understand that the information is subject to change.

Use of CHRI (Name-Based)

Access to the III System using name-based queries and record request messages is not permitted for noncriminal justice purposes, unless authorized pursuant to federal statutory authority or Compact Council regulations promulgated based upon federal statutory authority.

Coordination and Approval

Agencies must only leverage recognized/approved authorities for submission of name-based noncriminal justice III System queries and record request messages. Examples of such authorities include the Compact Council's Fingerprint Submission Requirements Rule (Purpose Code X), the Housing Opportunity Extension Act (Purpose Code H), and the Security Clearance Information Act (Purpose Code S). When applicable, agencies must coordinate with the FBI to determine specific requirements for use of a particular authority and obtain formal approval prior to use (e.g., Purpose Code X). When applicable, agencies must also obtain updated approval from the FBI for any changes associated with a previously approved authority.

Authorized Requests

Agencies must only submit name-based noncriminal justice III System queries and record request messages for authorized purposes covered by the authority leveraged for the request (i.e., federal statutory authority or Compact Council regulations promulgated based upon federal statutory authority). In addition, agencies must only submit requests for purposes that are known to exist at the time of submission. Agencies must not submit requests for a future anticipated need, even if the need is covered by an approved authority.

Implementation

Agencies must implement applicable administrative/procedural provisions required by the authority leveraged to submit name-based III checks for noncriminal justice purposes (e.g., follow-up fingerprints for Purpose Code X and limits on direct access by public housing authorities for Purpose Code H).

Re-use

Agencies must only use CHRI received as a result of noncriminal justice name-based III System queries and record request messages for the specific purpose originally requested. Agencies must not subsequently re-use CHRI for unrelated needs, even if the new needs are covered by a recognized/approved authority. Congruent with requirements for CHRI received as a result of fingerprint-based requests, re-use of CHRI received via name-based III checks may be acceptable in limited circumstances.

Dissemination of CHRI

The requirements for the dissemination of CHRI for noncriminal justice purposes are derived from various federal statutes, regulations, policies, and interpretations thereof, to include rules and procedures promulgated by the Compact Council. Primary references for these requirements include:

- Title 28, U.S.C., Section 534 (a)(4)
- Title 34, U.S.C., Section 40316, Article IV (c)
- Title 28, CFR, Section 20.33
- Title 28, CFR, Section 50.12
- Title 28, CFR, Section 906
- *III/NFF Operational and Technical Manual*, Chapter 3
- Compact Council's Noncriminal Justice Online Policy Resources

The NGI audit assesses three categories of requirements for dissemination of CHRI for noncriminal justice purposes: (1) Authorized Recipients, (2) Jurisdictional Control, and (3) Public Access. These categories center on the baseline requirement for allowable dissemination to receiving departments, related agencies, and other authorized entities. It should be noted that while the requirements below are written primarily from a state perspective, they also apply to federal and federally-regulated agencies that request, receive, and use CHRI for noncriminal justice purposes.

Authorized Recipients (Receiving Departments and Related Agencies)

CHRI may only be disseminated to receiving departments and related agencies that are authorized relative to the federal statutory authority used to obtain CHRI. States must ensure that recipients fall within allowable parameters established by federal statutory authorities leveraged for national criminal history checks.

As with the use of CHRI, parameters for dissemination are derived from the specific federal statutory authority leveraged to obtain CHRI. CHRI may only be disseminated to entities that are authorized relative to the federal statutory authority used to submit a fingerprint check. For example:

- Dissemination is limited to officials of state and local governments for CHRI obtained pursuant to Public Law 92-544.
- Dissemination is limited to "authorized agencies" defined as a division or office of a state for CHRI obtained pursuant to the NCPA/VCA. However, dissemination of CHRI is extended to nongovernmental qualified entities if a VECHS program is implemented.
- Dissemination is limited to the following entities for CHRI obtained pursuant to the Adam Walsh Act: 1) child welfare agencies, which include states, local agencies, other public agencies, or any other private agencies under contract with a state or local agency responsible for licensing or approval of foster or adoptive parents; and 2) public or private elementary or secondary schools as well as state and local educational agencies.
- Dissemination is limited to governmental agencies for CHRI obtained pursuant to the Serve America Act.

It is important to recognize that state or local laws, ordinances, administrative rules, or procedures may not be more permissive regarding dissemination of CHRI relative to the federal

authority used to obtain CHRI. However, states may be more restrictive and establish additional limitations on dissemination.

Receiving Departments

States should designate primary authorized recipients responsible for accessing or receiving CHRI directly from the state repository for noncriminal justice purposes. These agencies typically have statutory authority or regulatory obligations associated with making fitness determinations and/or providing oversight of the employment or licensing processes for particular categories of applicants. States must ensure that primary receiving agencies fall within parameters established by the federal statutory authorities being leveraged for national criminal history checks. CHRI may only be disseminated to entities that are authorized relative to the federal statutory authority used to obtain CHRI.

Depending upon the specific procedures used by a state, there may be multiple primary agency types with access to CHRI for a particular type of national criminal history check. For example, while one state's procedures may only include disseminating CHRI directly to a Department of Education for background checks of teachers, another state's procedures may include dissemination of CHRI directly to each local county school board. Still another state's procedures may include simultaneously disseminating CHRI directly to both the Department of Education and a local county school board.

The term "agency" encompasses offices, departments, bureaus, and other subdivisions associated with a particular agency's organizational structure. Although baseline dissemination requirements for CHRI are centered at the department and agency levels, as a best business practice, states should limit access to the minimum necessary sub-offices and personnel within a department or agency that are actually required for a particular use. While authorized receiving agencies may exercise some level of discretion and freedom of maneuver to distribute CHRI within their organizational structure, they should be able to demonstrate a reasonable need for doing so. For example, a local county school board may be designated as an authorized recipient of CHRI for the purpose of conducting background checks for prospective teachers. CHRI is stored as part of an electronic personnel records management system accessible by all school board employees. Although the school board is an authorized recipient, it is in the agency's best interests to limit access to CHRI on the system to only the personnel within the human resources department responsible for making fitness determinations. This will limit the school board's exposure to the inherent risks associated with unauthorized dissemination of CHRI.

Many statutory authorities leveraged for national criminal history record checks limit dissemination to governmental agencies. Most governmental agencies are readily identified, such as those statutorily designated, funded, and organized as part of a state's executive, legislative, and judicial branches. However, governmental entities, such as commissions and boards that may be comprised of political appointees, elected officials, and/or officials from private industry, may also qualify as authorized recipients of CHRI. Examples could include school boards and lottery commissions.

Related Agencies

Two primary categories of related agency exist with respect to dissemination of CHRI. The categories are based on the use of CHRI for a single need versus multiple needs, and are derived from historical definitions of related agency doctrine as well as standing audit practices and legal interpretations.

- *Dissemination of CHRI to related agencies for a single need/purpose.* This type of dissemination of CHRI occurs when multiple agencies are involved in making a single fitness determination associated with an application for a specific authorized noncriminal justice purpose, such as a license, position of employment, or benefit. In many instances, this type of related agency is a secondary recipient of CHRI from a primary agency that receives CHRI directly from the state level. The intent is to allow some level of flexibility within the allowable parameters established by the federal statutory authority being leveraged for the national criminal history check. For example, with the state's consent, the Department of Education and local county school boards are both involved in adjudication of teacher employment applications. In addition, on an ad-hoc basis, some of these local county school boards make CHRI available to their local Sheriff's Office in order to answer questions regarding specific charges on criminal history records. Another example includes, with the state's consent, the Bureau of Professional Licensing and the Real Estate Commission are both involved in adjudication of real estate license applications.
- *Dissemination of CHRI to related agencies for multiple needs/purposes.* This type of dissemination of CHRI occurs when multiple agencies are involved in making fitness determinations for separate but related needs associated with multiple applications for specific authorized noncriminal justice purposes, such as a license, position of employment, or benefit. This type of dissemination directly correlates to the re-use of CHRI for related needs as described in the Compact Council's online policy resource, *Use of FBI CHRI for Noncriminal Justice Purposes*. For example, if established requirements are met, there are limited instances when CHRI may be disseminated between agencies pursuant to the Public Law 92-544 Article IV sharing initiative or the NCPA/VCA VECHS program. However, just as CHRI must not be re-used for subsequent unrelated needs by the original requestor/recipient, it is imperative to recognize that CHRI must also not be disseminated to another recipient for subsequent unrelated re-use. In addition, CHRI may not be disseminated to another recipient for future anticipated uses, regardless of whether or not the needs are formally related.

Just as with the primary receiving agency, any related secondary recipient must also be authorized relative to the federal statutory authority used to obtain CHRI. For example, agencies related for the purpose of adjudicating an employment application for child day care pursuant to Public Law 92-544 must be governmental. Note that even though a private employer, such as a day care center, may be perceived as having a commonality of purpose, CHRI may not be disseminated to them by the governmental agency. States should be able to demonstrate a reasonable need for which they have designated agencies as related for the purpose of adjudicating a particular type of applicant.

It is important to recognize the distinction between authorized recipients, related agencies, and contractors. A related agency is essentially a specially designated authorized recipient with an inherent authority to access CHRI, and therefore does not require formal implementation of the Compact Council's *Security and Management Control Outsourcing Standard for Non-Channelers*. However, a governmental or private contractor has no such inherent authority, and therefore does require formal outsourcing implementation. Authorized recipients may not leverage outsourcing to create an authority for the intended purpose of designating an entity as a related agency. For example, pursuant to Public Law 92-544, local county school boards are typically considered to be related to the Department of Education; however, private schools would not be considered related agencies, because they are nongovernmental. As such, the Department of Education could not implement outsourcing to designate a private school as a "contractor" to allow the private school access to CHRI for the purpose of making fitness determinations on the private school's applicants. As an alternative, the state could consider leveraging the Adam Walsh Act or the NCPA/VCA VECHS program, both of which authorize dissemination to nongovernmental entities, thus designating such entities as authorized recipients.

Other Authorized Entities

For NGI audit purposes, other authorized entities represent assessments of specific requirements not directly assessed or reported as part of the Authorized Recipients category.

Jurisdictional Control

Agencies outside of a state's jurisdiction cannot be designated as related agencies, even when a congruent related need appears to exist for the use of CHRI. The dissemination restriction primarily centers on each state's individual authority and obligation to administer access to CHRI. Each state has the authority to determine whether or not to conduct particular types of noncriminal justice background checks, and each state is responsible for establishing the mechanisms and procedures for those checks within its jurisdiction. In addition, each state possess limited authority to meet obligations for maintaining appropriate controls, such as user agreements and audits, outside of its jurisdiction, especially with respect to another state's governmental agencies. In conjunction with the more obvious jurisdictional concerns associated with one state's governmental agency leveraging another state's statutes under Public Law 92-544, similar jurisdictional concerns also exist with the use of other statutory authorities such as the Adam Walsh Act or the NCPA/VCA. Examples of unauthorized dissemination include:

- One state governmental agency sharing CHRI with another state's governmental agency for adoption purposes when the child and prospective parents reside in different states, even if both states have approved Public Law 92-544 state statutes.
- Criminal history sharing initiatives involving participation in national compacts, associations, or databases such as those for child placement or employment/licensing in the health care industry.

This dissemination restriction is not intended to limit a state from making CHRI available in very limited situations to certain nongovernmental entities outside of the state's geographical boundaries when such dissemination is specifically authorized and formal jurisdictional authority is established to maintain adequate controls. It is very important to recognize that in order for dissemination to occur beyond a state's geographical

boundaries, there must first be an approved statutory authority which allows nongovernmental entities access to CHRI within the state's geographical boundaries. There must also be a recognized authority and obligation to formally establish security controls over the nongovernmental entities. For example, it is acceptable for a state to leverage an out-of-state private contractor for record archiving and destruction, since access to CHRI by private contractors is authorized pursuant to Title 28, CFR, Section 906, and jurisdictional authority for controls such as audits would be formally established through implementation of the *Security and Management Control Outsourcing Standard for Non-Channelers*.

Public Access

CHRI must not be disseminated to the general public. This includes maintaining CHRI in formats that are accessible by the public or within records that are subject to release through public record requests. However, CHRI may be disclosed as part of the adjudication process during a hearing that is open to the public if the agency demonstrates: 1) the hearing is based on a formally established requirement; 2) the applicant is aware prior to the hearing that CHRI may be disclosed; 3) the applicant is not prohibited from being present at the hearing; and 4) CHRI is not disclosed during the hearing if the applicant withdraws from the application process. For example, a board or commission may be authorized to access CHRI, and as part of regularly scheduled meetings, applicant appeals are discussed as standard agenda items. Even when the specific conditions are met to allow disclosure during a public hearing, the most preferable method for introducing CHRI is to enter into a closed session which limits participation by the public at large. States and local agencies should be able to reasonably demonstrate how the prerequisite criteria are being met for audit purposes.

Additional Considerations

Although not formal categories of assessment, the following considerations are applied to the assessment of requirements for dissemination of CHRI.

General

States need to maintain visibility on the full spectrum of primary agencies to which they disseminate CHRI, as well as the specific purposes/authorities for which those primary agencies receive CHRI. This is especially significant given the requirements for states to execute agency user agreements and establish formal noncriminal justice audit programs in accordance with the *CJIS Security Policy*.

Dissemination of CHRI is broader in concept than the simple act of physically or electronically sending CHRI to a recipient. The concept of dissemination also applies to making CHRI available to recipients through physical or electronic access. The overarching requirements associated with dissemination of CHRI apply regardless of whether CHRI is "pushed" to recipients or "pulled" by recipients since the end result is the same.

Notifications

The definition of CHRI includes information that confirms the existence or nonexistence of CHRI. This includes applicant status information, which is either directly attributed to or predominately based on a national FBI check, when no authority or inherent need

exists for the release of such information. However, if an inherent need does exist to advise a particular entity not otherwise authorized relevant to the federal statutory authority being leveraged for the national criminal history check, then it is acceptable to notify the entity of the outcome of applicant fitness determinations. Entities to which an applicant is seeking employment or licensing may receive status notifications which indicate the positive or negative outcome of fitness determinations. For example, a private day care center is not an authorized recipient of CHRI received pursuant to Public Law 92-544, but may be eligible to receive a status notification regarding an applicant who is seeking employment at the day care center (this assumes of course the approved state statute covers the employment type). States should be able to demonstrate the inherent need for which a particular entity is designated to receive status notifications. Status notifications must not contain CHRI to include confirming the existence or non-existence of CHRI. Generic “pass/fail” language must be used to the greatest extent possible, with the understanding that a reasonable balance must exist between the need to notify a potential employer and not indirectly confirming the existence or non-existence of CHRI. In addition, notification language should not directly reference that a national FBI check was conducted.

Subject of the Record.

Agencies may disseminate fingerprint-based CHRI obtained for noncriminal justice purposes to the subject of the record. It is important to note that agencies are under no direct obligation to provide CHRI to the subject, and dissemination of CHRI by local agencies to the subject may be limited at the state’s discretion. As a best business practice, agencies that disseminate CHRI to the subject of the record should verify the subject’s identity prior to dissemination and document each occurrence. Also, in order to limit potential risks associated with a subject’s subsequent use of a criminal history record, agencies may wish to consider marking the record in some manner to distinguish it as not an original copy.

CHRI may not be disseminated to spouses or other household or family members, even at the subject’s request. Further, CHRI may not be disseminated to other parties such as potential employers on behalf of the subject. However, although the preference is to disseminate directly to the subject of the record, a subject may request that their record be accessed by an attorney acting on the subject’s behalf. This scenario could potentially be encountered when an applicant challenges the outcome of an agency’s fitness determination as part of a formal appeal process.

Residual Access

Other authorized entities also include agencies which require residual access based on oversight authority and responsibility, such as the review of case files by an inspector general’s office or regulatory auditors from outside the receiving organization. Such access should be limited to only the minimum level necessary to accomplish oversight responsibilities, and controls should be established to reasonably prevent unauthorized disclosure of CHRI.

In limited circumstances, government agencies may also be related for the purpose of simply serving as a pass-through for fingerprints and receipt of CHRI. This typically occurs in situations when a criminal justice agency, such as a police department,

performs this specific function on behalf of an authorized recipient. The premise is that “access” to CHRI (view or make use of) is limited to such an extent to essentially consider it negligible for the purposes of formally categorizing it as access.

Purpose for Disclosure of CHRI

The Privacy Act of 1974 requires that the FBI’s CJIS Division keep an accurate accounting of the purpose of each disclosure of a criminal history record and the recipient of that record. (Title 5, U.S.C., Section 552a (c)(1)(A); *III/NFF Operational and Technical Manual*, Chapter 3, Section 2.1)

The NGI audit assesses three categories of requirements for the purpose for disclosure of CHRI: (1) Reason Fingerprinted Field, (2) III Purpose Codes, and (3) Reason for Request.

Reason Fingerprinted Field

All fingerprint-based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.

III Purpose Codes

All name-based III inquiry and record request messages must include the correct purpose code for which the CHRI is to be used.

Reason for Request

All users are required to provide the reason for all name-based and fingerprint-based III transactions upon request by CJIS systems managers, administrators, and representatives. While the purpose code and reason fingerprinted field provide some lead information, they only provide a minimal audit trail. Requiring the specific reason for all III inquiries assists the FBI in ensuring III transactions are conducted for authorized purposes and purpose codes and RFPs are being correctly used. There is also an obligation to ensure requests for CHRI are being conducted for only authorized purposes prior to the submission of the request to the FBI. Submitting entities (e.g., state repositories) are ultimately responsible for ensuring these requirements are met throughout their applicable jurisdictions and should develop the policies, procedures, training, and controls necessary to ensure compliance. While submitting entities should be in a position to indirectly provide or otherwise facilitate providing specific reasons for requests for CHRI during FBI audits, typically local agencies and/or organizational subcomponents that receive and directly use CHRI to adjudicate applications are in the best position to provide specific validating information regarding individual applicants.

Agency identifiers for receipt of CHRI

The inability of an agency to provide a specific reason may be the indirect result of other compliance issues. If an agency receives CHRI for an individual that it has no knowledge of, then there may actually be a dissemination issue. For example, if a state uses a livescan vendor who makes an inaccurate selection of an agency’s Originating Agency Identifier (ORI) or other similar identifier, then the state may send the results to the wrong agency. Unlike the agency that is legitimately waiting for the CHRI, the receiving agency has no knowledge of the applicant and is not able to provide a reason for the submission when asked to do so. As a best business practice, when an agency receives CHRI on an individual that is unknown to the agency, it should inform the state

repository. This practice allows the state repository the opportunity to find out what went wrong with the submission and to ensure that the correct agency is not waiting any longer than necessary for the results of the submission. Submitting entities should also establish effective policies, procedures, and other controls necessary to minimize the risk of inaccuracies with fingerprint submissions that result in the wrong agency receiving CHRI.

Independent application, fingerprinting, and adjudication processes

In a traditional process model, a single agency might be responsible for receiving an individual's application, fingerprinting the applicant, and adjudicating the results of the background check. However, variations on this model have been implemented by agencies, whereby processes associated with receiving an application, obtaining fingerprints, and adjudicating results are independent or "split" from one another and/or performed by a separate entity. These variations may result in applicants being fingerprinted prior to submitting an application. The receipt of fingerprints prior to the application may cause an agency's inability to reasonably assure that the CHRI was for a legitimate purposes and/or the agency may have no knowledge of the applicant. Separate application, fingerprinting, and adjudication processes do not necessarily cause a compliance issue, but oversight agencies must provide sufficient management control to ensure agencies within their jurisdictions that implement such processes have adequate visibility and controls in place to reasonably reduce the risk of unauthorized requests for CHRI and to be able to provide a specific reason for the CHRI request.

Documentation of reason for request

Although agencies must be able to provide CJIS Systems managers, administrators, and representatives some level of specificity about the requests for CHRI in order for them to be "known," there is no direct requirement for an agency to maintain "case files" or other documents in order to support requests for CHRI. In order to meet the requirements for providing a specific reason for requests for CHRI, agencies must have a reasonable level of knowledge of the subject and the specific reason for requesting CHRI for that subject and be able to provide sufficient supporting information, regardless of format. While this is typically accomplished by providing a copy of an application corresponding to a request for CHRI, there are other means by which agencies are able to meet this requirement. A few examples of items that may be used to provide supporting information include: information contained in a personnel database or other information system; copies of online registrations; e-mails showing the purpose or the applicant's position; and supporting statements from applicable officials.

Applicant Notification

Authorized governmental and non-governmental agencies/officials that conduct a national fingerprint-based criminal history record check on an applicant for a noncriminal justice purpose (such as employment or a license, immigration or naturalization matter, security clearance, or adoption) are obligated to ensure the applicant is provided certain notices and other information and that the results of the check are handled in a manner that protects the applicant's privacy. All notices must be provided in writing. These obligations are pursuant to the Privacy Act of 1974, Title 5, U.S.C., Section 552a, and Title 28, CFR, Section 50.12, among other authorities. Primary references for these requirements include:

-
- Title 5, U.S.C., Section 552a (e)(3)
 - Title 28, CFR, Section 50.12
 - Compact Council Meeting, November 2019, Topic 4, Privacy Notice Fundamentals
 - Compact Council Brochure, Agency Privacy Requirements for Noncriminal Justice Applicants

The NGI audit assesses two categories of requirements for applicant notification: (1) FBI Privacy Act Statement and (2) FBI Record Access and Amendment.

FBI Privacy Act Statement

The Privacy Act of 1974 (Title 5, U.S.C., Section 552a) was enacted to balance the government's need to maintain information about individuals with the right of individuals to be protected from unwarranted invasions of privacy. The Privacy Act regulates the government's collection, maintenance, use, and disclosure of records about individuals. It applies to all federal agencies, including the FBI, and it applies to all systems of records maintained by those agencies, including the NGI system.

Certain parts of the Privacy Act are especially relevant to the NGI system, the National Crime Prevention and Privacy Compact Council (Council), and noncriminal justice background checks. Subsection (e)(3) of the Privacy Act provides the basis for the notice requirement when noncriminal justice fingerprints are collected for submission to the NGI system. The text of (e)(3) is as follows:

- (e) Each agency that maintains a system of records shall-*
- (3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual-*
- (A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;*
- (B) the principal purpose or purposes for which the information is intended to be used;*
- (C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and*
- (D) the effects on him, if any, of not providing all or any part of the requested information.*

In order to comply with this section of the Privacy Act, the FBI requires that agencies must use the Privacy Act statement presented to, and approved by, the Council in 2013. This statement has been approved by the Office of Management and Budget (OMB) and is printed on the FD-258 fingerprint cards. This notice includes all of the required information, such as the authority, the principle purpose, and the routine uses. The Privacy Act statement is as follows:

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

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

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

The requirement for a Privacy Act statement for the submission of noncriminal justice fingerprints is not new; however, it has become of greater importance due to the retention of such fingerprints in the NGI system and the Rap Back service. Because a right, benefit, or privilege is being granted based on the information collected, it is essential that the individual knows that the submission of his or her information is voluntary and knows what will happen with the information once it is submitted. The OMB, the agency that promulgates Privacy Act guidance and directives for the federal government, has opined that implicit in subsection (e)(3) is the idea of "informed consent", meaning that the individual should be provided with sufficient information to make an informed decision on whether to provide his information to the government.

Contributors of noncriminal justice fingerprints to the NGI system have inquired as to what constitutes a sufficient or adequate Privacy Act statement. The FBI requires that agencies use the current (i.e. 2013 or later) FBI Privacy Act statement, with additional language as necessary for state or federal agency purposes. If the agency does not use the exact language of the FBI Privacy Act statement, it must use language that is substantively similar to the FBI language. At a minimum, the language must address the submission of the fingerprints and associated information to the NGI system; the searching of the fingerprints against the civil, criminal, and latent repositories; and the continual comparison of the fingerprints to other fingerprints submitted to or retained by the NGI system.

Contributors of noncriminal justice fingerprints to the NGI system have requested clarification on best practices for providing the Privacy Act statement and how to effectively document those practices for auditing purposes. Since the Privacy Act was passed decades before our current electronic systems, it is important to comply with the statute but to also accommodate modern technology. In its Circular A-108, "Federal Agency Responsibilities for Review, Reporting, and

Publication Under the Privacy Act”, OMB stated that a Privacy Act statement is necessary “regardless of whether information is collected on a paper or electronic form, on a website, on a mobile application, over the telephone, or through some other medium”.

In past guidance to the Council, the FBI has advised that the Privacy Act statement must be provided in writing in order to comply with the statute, and that the notice may be provided in hard copy or in electronic format. For example, the notice may be provided on the hard-copy fingerprint card, on a form included with an application package, via an electronic notice on a live scan machine, or an electronic notice that must be viewed by the applicant before proceeding with the application. The agency must demonstrate that each individual received the Privacy Act statement. The FBI requires that the contributors have a verifiable process in place to ensure that all individuals have received the requisite Privacy Act statement. Simply providing a general notice, such as a poster on a wall or a notice on a website, will not be sufficient. The Privacy Act statement should be provided before or at the time of collection of the fingerprints in order to ensure informed consent and a copy should be provided to the individual if he or she requests it.

Contributors also have inquired as to how long they should maintain proof of having provided the Privacy Act statement to individuals. The FBI recommends that each agency follow its own record retention rules; however, the contributor will need to document the verifiable process to the CJIS Audit Unit when requested and for participation in Rap Back.

In the Spring of 2017, the “Noncriminal Justice Applicant’s Privacy Rights” and “Agency Requirements for Noncriminal Justice Applicants” brochures were modified to include an “acknowledgement” on the part of the individual receiving the Privacy Act statement. Although it would be a good practice for the individual to acknowledge receipt of the Privacy Act statement (e.g. the applicant checks a box on the live scan screen to confirm receipt of the notice), there is no requirement for the relevant agency to require or maintain such acknowledgements. Individual acknowledgments would certainly assist with documenting Privacy Act compliance and informed consent, but the statute requires that agencies provide the individual notice, not that the individual acknowledges receipt of that notice.

FBI Record Access and Amendment (28 CFR 50.12)

Subsection (d) of the Privacy Act contains the access and amendment provisions that require each federal agency that maintains a system of records to, upon request, permit the individual to gain access to his record or any information pertaining to him in the system and review the record and have a copy made. The Privacy Act also has procedures for an individual to request correction of his record if he believes it is not accurate, timely, relevant, or complete, and provides procedures if his request for correction is denied.

For access and amendment of criminal history records, the Department of Justice issued specific regulations found at 28 CFR 16.30-16.34 that require the individual to submit fingerprints, an application with certain biographic information, and a fee. If seeking a change, update, or correction to his or her record, the individual is generally directed to the agency that contributed the information to the FBI. This process is known as the “Departmental Order” process and has been briefed to the Council for many years. The “Departmental Order” process whereby an individual requests a copy of his or her criminal history record is simply the specific means by which the Privacy Act rights of access and amendment are implemented for criminal history records.

Another federal regulation, 28 CFR 50.12, requires that applicants receive notice that their fingerprints will be searched in the FBI's system and must be advised of their rights to seek a change, correction, or updating of their records pursuant to 28 CFR 16.34. The relevant text of 28 C.F.R. 50.12 is as follows:

Officials at the governmental institutions and other entities authorized to submit fingerprints and receive FBI identification records under this authority must notify the individuals fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. The officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of an FBI identification record are set forth in 28 CFR 16.34. Officials making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so. A statement incorporating these use-and-challenge requirements will be placed on all records disseminated under this program. This policy is intended to ensure that all relevant criminal record information is made available to provide for the public safety and, further, to protect the interests of the prospective employee/licensee who may be affected by the information or lack of information in an identification record.

If the applicant receives the current Privacy Act statement, the notice requirement of 28 CFR 50.12 regarding searching of the fingerprints to check the criminal history records of the FBI has been met. However, the agency also must be certain to provide written notice to the applicant regarding the procedures for accessing and amending his or her criminal history record. All applicants must be provided with such notice, regardless of whether the applicant, in fact, has any criminal history record information in NGI. The FBI recommends that agencies provide both the Privacy Act statement and the 28 CFR 50.12 notice at the same time and/or on the same document if possible, to ensure that the applicant receives all required notices.

In addition to the notice requirements of 28 CFR 50.12, the regulation requires that applicants must be afforded the opportunity to correct or complete criminal history records. This opportunity must be afforded whether the criminal history is actually used to disqualify the applicant or not. The CJIS Audit Unit ensures that agencies have a verifiable process in place to comply with this requirement.

28 CFR 50.12 states that applicants should not be denied employment or licensing based on information in the criminal history record until they have been afforded a reasonable time to correct or complete the record, or declined to do so. At Council meetings in 2011, the question of what constituted a "reasonable" time was discussed and the Council declined to define the term. The FBI does not consider this part of 28 CFR 50.12 to be a requirement because it states that officials "should" (rather than "must" or "shall") not deny employment or licensing. While it would be a best practice to have up-to-date and accurate criminal history information before making employment decisions, the FBI recognizes that many other considerations and limitations affect the hiring/licensing decisions.

Additional Considerations

The FBI recommends that agencies consult the “Noncriminal Justice Applicant’s Privacy Rights” and “Agency Requirements for Noncriminal Justice Applicants” brochures to ensure that all of the requirements pursuant to the Privacy Act and 28 CFR 50.12 are being met.

The FBI has no objection to officials providing a copy of the applicant’s FBI criminal history record to the applicant for review and possible challenge when the record was obtained based on positive fingerprint identification. If agency policy permits, this courtesy will save the applicant the time and additional FBI fee to obtain his/her record directly from the FBI by following the procedures found at 28 CFR 16.30 through 16.34. It will also allow the officials to make a more timely determination of the applicant’s suitability.

Each agency should establish and document the process/procedures it utilizes for how/when it gives the applicant the FBI Privacy Act statement, the 28 CFR 50.12 notice, and the opportunity to correct his/her record. Such documentation will assist State and/or FBI auditors during periodic compliance reviews on use of FBI criminal history records for noncriminal justice purposes.

Noncriminal Justice Agency Audits

Each CJIS Systems Agency, in coordination with the State Identification Bureau, shall establish a process to periodically audit all noncriminal justice agencies, with access to Criminal Justice Information, in order to ensure compliance with applicable statutes, regulations and policies. (*CJIS Security Policy, Section 5.11.2*)

User Fee

Agencies must ensure fingerprint-based requests for CHRI are properly submitted in order to ensure the appropriate application of user fees. Pursuant to Public Law 101-515, the FBI may establish and collect fees to process fingerprint identification records and name checks for noncriminal justice, non-law enforcement employment and licensing purposes.

The NGI audit assesses two categories of requirements for user fee: (1) Criminal Justice and (2) Volunteer.

Criminal Justice (No-fee)

Processing of fingerprint submissions for screening criminal justice agency employees or applicants for employment (sworn and non-sworn) are at no cost inasmuch as criminal justice employment is considered an administration of criminal justice function. (Title 28, CFR, Section 20.33 (a)(1))

In addition, processing of fingerprint submissions for screening those under contract with criminal justice agencies are at no cost under the following circumstances:

- The contractor is providing services for the administration of criminal justice.
- The contractor is performing services unrelated to the administration of criminal justice, but has unsupervised access to the facility (criminal justice agency site security).

However, fingerprint submissions for screening employees of contractors to whom the entire administration of criminal justice functions have been outsourced, such as private prisons and emergency dispatch centers, are subject to the user fee.

(*Criminal Justice Contract Employee Fingerprint Submission Summary Sheet*, September 2, 2003 and *CJIS Information Letter 07-1*, January 8, 2007)

It should be noted that the definition of “administration of criminal justice” appearing at Title 28, CFR, Section 20.3 (b) includes “Detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders.” However, it is recognized that there are other services which must be performed in support of these nine identified functions and hence, would also be considered an administration of criminal justice function. For example, personnel who transport, feed, provide medical (including psychiatric) care, teach and otherwise engage in the rehabilitative process also perform an administration of criminal justice function, although their functions are only implicitly contained within the regulatory definition.

Volunteer (Reduced-fee)

In the case of a background check conducted with fingerprints on a person who volunteers with a qualified entity, the fees collected by the FBI may not exceed eighteen dollars, or the actual cost, whichever is less. The Type of Search Requested field for applicable fingerprint submission transaction types must be set to a value of “V” to ensure proper processing.

(Title 34, U.S.C., Section 40102 (e); *Electronic Biometric Transmission Specification*, version 10.0.9, Appendix C, page C-40)

Abbreviation or Acronym	Term
Adam Walsh Act	Adam Walsh Child Protection and Safety Act
CFR	Code of Federal Regulations
CHRI	Criminal History Record Information
CJIS	Criminal Justice Information Services
Compact	National Crime Prevention and Privacy Compact
Serve America Act	Edward M. Kennedy Serve America Act
FBI	Federal Bureau of Investigation
III	Interstate Identification Index
NCPA/VCA	National Child Protection Act/Volunteers for Children Act
NFF	National Fingerprint File
NGI	Next Generation Identification
ORI	Originating Agency Identifier
U.S.C.	United States Code
VECHS	Volunteer and Employee Criminal History System
WAN	Wide Area Network