# BULLETIN

**No. 2020-2** **February 18, 2020**

**Subject: Fingerprint processing - applicant Privacy Act rights and protecting CHRI**

The NIGC processes fingerprints submitted by tribes for background investigations of primary management officials (PMO) and key employees (KE). Prior to issuing a gaming license to a PMO or KE, a tribe is required to perform a fingerprint check through the FBI records system as part of the background investigation on each applicant. The criminal history record information (CHRI) obtained as a result of the check assists the tribe in determining the applicant's eligibility for employment.

This bulletin discusses the requirements for fingerprint processing: notifying applicants of their Privacy Act rights, their opportunity to complete or challenge information in their FBI identification record, and the process by which they may obtain a change, correction, or update to such record. This bulletin also details the requirements for protecting and using CHRI, including summaries of it, and complying with the FBI's CJIS Security policy. The FBI and/or NIGC will audit Tribes' compliance with these requirements as set forth here and in each Tribe's Memorandum of Understanding (MOU) with the NIGC.

## Applicant Privacy Act rights

### 1. *Applicant record notification / NCJA Privacy rights notice*

Prior to taking a PMO/KE applicant's fingerprints, tribes must provide these applicants with the written *Applicant Record Notification* - also known as the Non-Criminal Justice Applicant's Privacy Rights notice. It may be given to the applicant electronically or in paper form. A copy of the notice is attached to this Bulletin.

This notice includes multiple requirements. First, it explains that the applicant's fingerprints will be used to check FBI's criminal history records. Second, if a criminal history record exists concerning the applicant, the TGRA needs to give them an opportunity to complete or challenge the information in the record. Third, the TGRA has to advise the applicant in writing that the procedures for obtaining a change, correction, or update of the record are set forth in Title 28, Code of Federal Regulations (C.F.R.) §16.34. Finally, the TGRA must afford the applicant a

reasonable amount of time to correct or complete the record (or decline to do so) before denying a gaming license based on information in the record.[1]

To facilitate the challenge/correction process, NIGC permits TGRAs to supply the applicant with a copy of their FBI criminal history record for review and possible challenge, correction, or update. This courtesy saves the applicant the time and additional fee required in obtaining the record directly from FBI. As a prerequisite, however, TGRAs must develop a written procedure for such releases. This written procedure must require verification of the applicant's identity prior to dissemination and must document each release. To limit potential risks associated with an applicant's subsequent use of CHRI, TGRAs need to mark the record in some manner to distinguish it as a copy, not the original. Although the preferred method is to release CHRI directly to the applicant, the record may be released, at the request of the applicant, to an attorney acting on their behalf. This scenario could arise as part of a formal appeal process, when an applicant challenges the outcome of the TGRA's eligibility determination. CHRI may not be disseminated to spouses or other household or family members, even at the applicant's request. And CHRI may not be disseminated to other parties such as potential employers or licensing agencies on behalf of the applicant.

If, however, the TGRA chooses not to provide the applicant a copy of the record, the TGRA's policy should prohibit its release for such purpose. And that policy must direct the applicant to the FBI's process for obtaining a copy, which is set forth at 28 C.F.R. §§16.30 - 16.34 and on the FBI's website, https://www.fbi.gov/services/cjis/identity-history-summary-checks.

### 2. *FBI Privacy Act Statement*

Also prior to submitting their fingerprints, PMO/KE applicants shall receive the FBI's Privacy Act Statement. The FBI's Privacy Act Statement is separate from the Privacy Act notice required under NIGC regulations[2], and a copy is attached to this Bulletin. Essentially, it informs applicants that their fingerprints will be used to check their criminal history records at the FBI.

### 3. *Both must be provided before fingerprinting*

Regardless of what entity a TGRA uses to submit fingerprints to the FBI, NIGC, or another source, the FBI requires that the Applicant Record Notification / NCJA Privacy rights notice and the FBI Privacy Act Statement be provided to all PMO/KE applicants prior to the applicant providing their fingerprints for a national criminal history records search.

FBI may update these notices periodically. Please check FBI's website for updates of the notices:

https://www.fbi.gov/services/cjis/compact-council/privacy-act-statement

https://www.fbi.gov/services/cjis/compact-council/guiding-principles-agency-privacy-requirements-for-noncriminal-justice-applicants

[1] *See* 28 C.F.R. § 50.12(b).
[2] 25 C.F.R. § 556.2.

## CHRI Use and Protection

### 1. *CHRI*

CHRI means information collected by criminal justice agencies about individuals, consisting of identifiably descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release.

CHRI also includes information that is transferred or reproduced directly from CHRI or information that confirms the existence or nonexistence of CHRI. CHRI includes any media that contains it, such as: Letters, emails, documents, notes, conversations – in person or via phone/text, and spreadsheets or tables. Examples of CHRI potentially include: notice of results (NORs), investigative reports (IRs), licensing objection letters, and other summaries of CHRI.

### 2. *Using and protecting CHRI*

CHRI is highly sensitive information – tribes, therefore, must take steps to ensure that it is used only for authorized purposes and securely maintained. CHRI may only be used to determine a PMO/KE applicant's eligibility for employment in the tribe's gaming operation, not for any other purpose. To be clear, "official use" of CHRI for licensing purposes is limited to those individuals performing work functions for, or managing, the gaming operation who come within the NIGC regulatory definitions of a PMO or KE, as set forth in 25 C.F.R. §§ 502.14 (a) – (c) and 502.19 (a) – (c).

All CHRI access must be restricted to tribal personnel directly involved in the licensing deliberations. And tribes shall maintain records of all persons accessing CHRI, which will be furnished to NIGC upon request. CHRI cannot be improperly disseminated beyond tribal personnel directly involved in licensing deliberations or reused.

Regarding reuse, CHRI obtained under an NIGC MOU cannot be shared with state gaming agencies for state licensing purposes. In most instances, CHRI made available via NIGC fingerprinting cannot be provided to tribal leadership, other tribal agencies beyond the TGRA, human resources, etc., to save money or to meet tribal-state gaming compact requirements. And although the use of CHRI may be necessary, and authorized under separate authority, to satisfy state licensing requirements, a new record request to the FBI through a non-NIGC process must be made in such instance.

However, regulatory inspections by a state gaming agency where they access CHRI as part of an audit or review of licensing during a site visit is not reuse and not prohibited. Neither are reviews by agencies that require residual access based on oversight and authority, such as an inspector general's office reviewing case files. But such access should be limited to only the minimum level necessary to accomplish oversight responsibilities and controls should be established to reasonably prevent unauthorized CHRI disclosure. Similarly, CHRI and its summary information may be disclosed in tribal proceedings related to KE/PMO eligibility determinations, but not in courts or administrative hearings without NIGC's prior consent.

### 3. *FBI's CJIS Security policy and compliance audits*

The FBI's Criminal Justice Information Services (CJIS) Division issued the CJIS Security policy to protect Criminal Justice Information[3] (CJI) and, its subset, CHRI. The policy applies to every individual and entity accessing CJI and CHRI, detailing operational and information security requirements for protecting transmissions and storage of it - including the hardware, software, and infrastructure used to receive, transmit, and store it. The policy also contains directives on how CJI and CHRI shall be maintained, viewed, accessed, processed, released, and destroyed and the training and authorizations needed for those individuals that do so.

All tribes accessing CHRI through NIGC must agree to comply with the policy and implement its requirements as detailed in their NIGC MOUs and the policy itself. Tribes will be subject to annual audits, including information technology security audits, by the NIGC to ensure compliance with the NIGC MOU and the FBI's CJIS Security policy. The FBI may also audit the Tribes, and such audits would likely occur once every three years.

**Training**

The NIGC has updated its training modules for backgrounding, licensing, and understanding CHRI. It includes the definitions of CHRI, applicants' rights, CHRI use, and CHRI reuse. It also includes CJIS Security Awareness training, which is required under the CJIS Security policy. Please see the CJIS Training materials on the NIGC website: https://www.nigc.gov/compliance/CJIS-Training-Materials . And a video entitled "NIGC Fingerprint Program Updates" covers information about updates to the NIGC fingerprint process and to the tribal background and licensing process, as well as the handling of FBI CHRI: http://bit.ly/CJISvideo

**New MOU**

In order to ensure compliance with the above requirements, each tribe receiving CHRI via the NIGC has to execute a new Memorandum of Understanding (MOU) - on or before January 1, 2021. Like the current MOU, the new one limits CHRI's use, including any summary of it, to tribal eligibility determinations for KE/PMO employment. As always, the new MOU, similar to the old, underscores FBI's right to impose additional restrictions on the release and use of CHRI beyond those set by the NIGC and reserves NIGC's right to discontinue providing CHRI where a tribe fails to comply with the MOU's terms.

[3] CJI is the term used for FBI CJIS provided data necessary for law enforcement and civil regulatory agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.