NIGC Fingerprint Program Update

Updated 2/24/2020
Today’s Topics

- The History of the Fingerprint Based Criminal History Searches
- What is a Criminal History Report Information
- Who’s Fingerprints can be submitted through the NIGC
- What FBI Notices are required to be given to gaming license applicants
Today’s Topics continued

- Policies required by FBI regarding applicant’s rights
- FBI restrictions on re-use of CHRI
- Updated guidance on Not Licensed by Tribe notifications to the NIGC under 25 CFR 558.3(d)
• NIGC and FBI entered into a MOU to process name searches – June 16, 1993.
• FBI Policy on IGRA Submissions by NIGC, States and Tribes – circa 1993.
The National Crime Prevention and Privacy Compact Act passes in 1998:

- Establish a uniform, nationwide standard governing the interstate dissemination of criminal history records for noncriminal justice purposes;
- Ensure the State and Federal agencies receive criminal records for authorized employment and licensing purposes; and
- Establish technology standards, supporting consistency and uniformity, increasing data sharing and integration.
Criminal Justice Information (CJI) is the term used to refer to all of the FBI Criminal Justice Information Services (CJIS) provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

Part of the CJI information is the CHRI report used for key employee and primary management official licensing.
Criminal History Record Information
Often referred to as a
“RAP sheet”

CHRI, a subset of CJI, is information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release.
Letters, emails, documents, notes, conversations in person/phone, and databases (including spreadsheets or tables) that contain:

Information transferred or reproduced directly from CHRI.

Information that confirms the existence or nonexistence of CHRI.

Regardless of its form, use, or method of dissemination, CHRI requires protection throughout its life cycle.
The FBI authorizes NIGC to disseminate CHRI to tribal gaming authorities solely for determining a PMO or KE applicant’s eligibility for a gaming license.

The FBI limits the dissemination of CHRI obtained through NIGC for only those applicants who will be employees of the gaming operation.

CHRI must be reviewed before a final licensing decision is made.
Who gets a background and license?

- Key Employees of the gaming operation
- Primary Management Officials of the gaming operation
PRIOR TO FINGERPRINTING

• Ensure applicant receives the Noncriminal Justice Applicant’s Privacy Rights Notice.


• Ensure applicant receives the FBI Privacy Act Statement.

  www.fbi.gov/services/cjis/compact-council/privacy-act-statement
CHRI POLICY

• TGRA must have a policy through which applicants may request and receive a copy of their CHRI.

• Applicants must be given time to correct or challenge information in the CHRI before the license eligibility determination is made.
CHRI Use Restrictions

• Do not disseminate any form of CHRI outside of those directly involved in the licensing process at the Tribe and NIGC.

• In most instances, CHRI obtained for PMO or KE licensing purposes cannot be provided to other entities for other purposes. CHRI cannot be provided to tribal leadership, other tribal agencies, state agencies, human resources, external auditors*, etc., for other purposes such as to save money or to meet tribal state gaming compact requirements.
Recent Notices from NIGC

- July 1, 2019 – Letter summarizing information above.

- July 19, 2019 – Letter requiring immediate discontinuation of fingerprinting of TGRA employees and Commissioners.
• 558.3(d) – If the tribe does not license an applicant:
  – Notify NIGC no license was issued; and
  – Forward the eligibility determination and NOR.

The background, eligibility determination and NOR are complete, but for any reason the applicant was not licensed, you must notify NIGC.

Can I still send in a NOR indicating not licensed even if we did not reach the eligibility determination stage? Yes, if you want to.

It will not consider it a missing NOR for 556 & 558 purposes if you do not.
• More information on the Compact Council
  – https://www.fbi.gov/services/cjis/compact-council

• For a copy of the CJIS Security Policy
Appendix G: Best Practices
- Cloud, Mobile Devices, Encryption, BYOD, Setting Access and Incident Response.

- Lists out the main sections of the policy that apply to NCJAs.
CJIS Security Policy – Key Areas

- Agreements
- Dissemination
- Security Awareness Training
- Incident Response
- Auditing and Accountability
- Access Control
- Media Protection
- Physical Protection
• Level 1: Baseline security awareness training for all personnel who have unescorted access to a physically secure location.
• Level 2: Security awareness training for all authorized personnel with physical access to Criminal Justice Information (CJI).
• Level 3: Security awareness training for all authorized personnel with both physical and logical access to CJI.
• Level 4: Security awareness training for all Information Technology personnel (system administrators, security administrators, and network administrators, etc.).
• Criminal Justice Information (CJI) must be encrypted:
  – When stored (at rest) outside the boundary of a physically secure location
    • When encryption is used for CJI at rest, it must be FIPS 140-2 certified and use a symmetric cipher of at least 128 bit in strength or use the AES symmetric cipher at 256 bit strength.
  – Immediately when transmitted outside the boundary of a physically secure location (two exceptions: 5.13.1.2.2 and 5.10.2)
    • When encryption is used for CJI in transit, it must be FIPS 140-2 certified and use a symmetric cipher of at least 128 bit.
CJIS Security Policy Exceptions for Encryption In Transit

Two exceptions as written in sections 5.13.1.2.2 and 5.10.2 are detailed as follows:

• Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements when an officer determines there is an immediate need for the CJI to further an investigation or situations affecting the safety of an officer or the general public.

• CJI transmitted via a single or multi-function device (fax) over a standard telephone line is exempt from encryption requirements.
In order for any third party (including Tribe’s IT) to have access to CHRI you must have an Outsourcing Agreement:

- Send letter to CJIS Compliance Officer requesting approval.
- Execute Contract.
- Inspect in 90 days.
Letter and Contract

REQUEST LETTER

FOOD AND THE (Name) TIDAL GATING COMMISSION (TGC)

[Contractor’s Name] AS A CONTRACTOR

FOR NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS

October 8, 2019

Mrs. Claudia S. Anderson
Contract Officer, FHWA Mobility D1
1000 Camelot Dr. Northbrook
Chicago, IL 60063-2966

Dear Mrs. Anderson:

The Tidal Gating Commission, the Authorized Recipient, requests permission to use the [Contractor’s Name] as a contractor to enhance noncriminal justice administrative functions relating to the processing of criminal history record information (CHRI) in its behalf. This would include all functions that may apply, for example,

- Obtaining noncriminal background information, making determinations and recommendations, offering services of current history record information and its corresponding fingerprint submissions, etc.

The Tidal Gating Commission and the [Contractor’s Name] are considering entering into an agreement with [Contractor’s Name] to enter into the [Tidal Gating Commission’s Name] Commission’s program in accordance with the Security and Management Control Outsourcing Standard (Outsourcing Standard) on the Tidal Gating Commission.

The Tidal Gating Commission is committed to performing background checks pursuant to Title 28 United States Code (U.S.C.), § 578, et al., as well as to the “Federal Bureau of Investigation” (FBI). Specifically, the National Information Sharing System (NICE) is a repository of noncriminal background checks that are conducted by the Tidal Gating Commission on behalf of the Tidal Gating Commission for federal and state law enforcement officials who processes all fingerprint information.

The Tidal Gating Commission will enter into a contractual agreement with the Contractor, in accordance with the Outsourcing Standard for Non-Criminal and the Criminal Justice Information Services (CJIS) Security Policy. However, the Contractor shall be required to meet any other standards established by the FHWA Contract Officer, subject to receipt of the written agreement.

The Authorized Recipient shall notify the FHWA Contract Officer that an audit was conducted with the Contractor within 30 days of the date the Contractor submitted the CHRI under the approved outsourcing agreement.

The Contractor agrees to: provide written notification to the FHWA Contract Officer as soon as possible. All records of the Tidal Gating Commission held by the Contractor shall be retained or destroyed in accordance with the Outsourcing Standard and the FBI Security Policy, and employees of the Contractor will continue to be authorized access to the CHRI records of the Authorized Recipient.

Upon execution of the Contract, the Contractor shall be responsible for [Contractor’s Name] compliance with the terms of this contract, to include the Outsourcing Standard for Non-Criminal and will notify the FHWA Contract Officer of any violations.

Sincerely,

[Contractor’s Name]

[Contractor’s Address]

[Contractor’s Phone Number]

[Contractor’s Email Address]

[Signature]

[Signature]

[Signature]

[Signature]

[Signature]
Under Part 2.05 of the Outsourcing Standard, the TGRA shall conduct an audit of the contractor within 90 days of the date the contractor first receives the FBI CHRI under the approved agreement and shall certify to the FBI Compact Officer it was conducted.
The Cloud

• At https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center:
  – Cloud Computing Report
    • Recommendations for Implementation
  – Cloud Report

• Appendix G of CJIS SP
  – See Cloud Computing
Over the next two years, the NIGC and the FBI will be working to migrate the NIGC’s policies on the use and dissemination of CHRI from our last/previous agreement with the FBI established in 1993 to include additional applicable standards and protocols established under the National Crime Prevention and Privacy Compact Act of 1998, the National Crime Prevention and Privacy Compact Council and the CJIS Security Policy.
Questions?

Contact Information:
TrainingInfo@nigc.gov