

# **National Indian Gaming Commission Noncriminal Justice Compliance Program**



## **Noncriminal Justice Agency Guide for Federal Criminal History Checks**

Document Updated: March 11, 2020

# Table of Contents

<b>Introduction</b>	<b>5</b>
<b>Contact List</b>	<b>6</b>
<b>Section 1 General Overview</b>	
<b>1.1</b> NIGC Overview	<b>7</b>
<b>1.2</b> Memorandum of Understanding	<b>7</b>
<b>1.3</b> Authorizations and Access	<b>8</b>
<b>1.3.1</b> Application for Access	<b>8</b>
<b>1.3.2</b> Noncriminal Justice Access	<b>8</b>
<b>1.4</b> Outsourcing Agreements	<b>9</b>
<b>1.4.1</b> Outsourcing Agreement Submission	<b>9</b>
<b>1.4.2</b> Contract Regarding Outsourcing Noncriminal Justice Functions	<b>9</b>
<b>Section 2 Fingerprint Submissions &amp; Results</b>	
<b>2.1</b> NIGC Fingerprinting Process	<b>11</b>
<b>2.1.1</b> Fingerprint Criminal History Check Process	<b>11</b>
<b>2.2</b> Applicant Identification	<b>11</b>
<b>2.3</b> FBI Applicant Privacy Rights Notifications and Privacy Act	<b>12</b>
<b>2.4</b> Electronic (Live Scan) Fingerprint Submission System Connectivity	<b>12</b>
<b>2.5</b> Mail Reply(s)	<b>13</b>
<b>2.6</b> System Testing	<b>13</b>
<b>2.7</b> Step by Step Transaction Flow(s)	<b>13</b>
<b>2.8</b> Basic Hard Card Fingerprinting Tips	<b>15</b>
<b>2.9</b> Protection of the Fingerprint Card Prior to Submission	<b>17</b>
<b>2.10</b> Required Information for Each Fingerprint Card Submission	<b>17</b>
<b>2.10.1</b> Fingerprint Card Legend	<b>17</b>
<b>2.11</b> Example Fingerprint Card	<b>20</b>
<b>2.12</b> Payment and Submission Packets	<b>20</b>
<b>2.12.1</b> Fees	<b>20</b>
<b>2.12.2</b> Payment Submittal Requirements	<b>21</b>
<b>2.13</b> Rejected Fingerprint Cards/Resubmissions	<b>21</b>
<b>2.13.1</b> Routine Name Search Procedure	<b>21</b>
<b>2.13.2</b> Example Individual FBI Reject Notice	<b>22</b>
<b>2.14</b> Example FBI Criminal History Record	<b>23</b>
<b>Section 3 Basic Privacy &amp; Security Guidelines</b>	
<b>3.1</b> Policies and Procedures	<b>34</b>
<b>3.2</b> Applicant Process	<b>35</b>
<b>3.3</b> Applicant Review and Challenge of Criminal History	<b>35</b>
<b>3.4</b> Communication/Dissemination	<b>36</b>
<b>3.4.1</b> Communication Cautions	<b>36</b>
<b>3.4.2</b> Secondary Dissemination	<b>37</b>
<b>3.5</b> Physical Security	<b>37</b>
<b>3.5.1</b> Storage	<b>37</b>
<b>3.5.2</b> Destruction	<b>38</b>

<b>3.6</b>	Technical/Digital Security	<b>38</b>
<b>3.7</b>	Consequences for Misuse	<b>39</b>
<b>Section 4 LASO Responsibilities</b>		
<b>4.1</b>	Primary Liaison	<b>41</b>
<b>4.1.1</b>	Information Changes	<b>41</b>
<b>4.1.2</b>	Authorized Personnel List	<b>42</b>
<b>4.2</b>	Privacy and Security Coordinator	<b>42</b>
<b>4.2.1</b>	Required Training for Authorized Personnel	<b>42</b>
<b>4.2.2</b>	Acknowledgement Statements	<b>43</b>
<b>4.3</b>	Audit Responsibilities	<b>43</b>
<b>Section 5 Audits &amp; Compliance</b>		
<b>5.1</b>	Audits	<b>44</b>
<b>5.1.1</b>	Routine Audits	<b>44</b>
<b>5.1.2</b>	Directed Audits	<b>44</b>
<b>5.2</b>	Compliance Review	<b>45</b>
<b>5.2.1</b>	General Administration	<b>45</b>
<b>5.2.2</b>	Fingerprint Submissions	<b>46</b>
<b>5.2.3</b>	Privacy and Security	<b>47</b>
<b>5.2.4</b>	Training	<b>48</b>
<b>5.2.5</b>	Key Employee and Primary Management Official Checklist	<b>48</b>
<b>5.2.6</b>	Gaming Operation Definition	<b>48</b>
<b>5.2.7</b>	Key Employee Definition	<b>48</b>
<b>5.2.8</b>	Primary Management Definition	<b>49</b>
<b>5.3</b>	National Identity Services Audit	<b>49</b>
<b>5.4</b>	Information Technology Security Audit	<b>50</b>
<b>5.4.1</b>	Noncriminal Justice Audit	<b>50</b>
<b>5.4.2</b>	Outsourcing/Channeling Audit	<b>50</b>
<b>Section 6 NIGC Classes &amp; Assistance</b>		
<b>6.1</b>	Initial Access & NCJA Compliance Training	<b>51</b>
<b>6.2</b>	Types of Training Offered by the NIGC	<b>51</b>
<b>6.3</b>	Requesting Site Specific Training from the NIGC	<b>51</b>
<b>6.4</b>	Other Training Options	<b>52</b>
<b>Section 7 First Steps to Achieve Compliance</b>		
<b>7.1</b>	How to Achieve Compliance	<b>53</b>
<b>References</b>		<b>55</b>
<b>Acronym Glossary</b>		<b>56</b>
<b>Appendix A</b>	<b>Memorandum of Understanding</b>	<b>57</b>
<b>Appendix B</b>	<b>Select Pages from the FBI Outsourcing Standards</b>	<b>60</b>
<b>Appendix C</b>	<b>FBI Required Privacy Act and Noncriminal Justice Applicants Rights Notice</b>	<b>78</b>
<b>Appendix D</b>	<b>NIGC Fingerprint System Security, Protocols and Data Requirements</b>	<b>80</b>
<b>Appendix E</b>	<b>CJIS Name Search Request Form</b>	<b>85</b>
<b>Appendix F</b>	<b>Sample Policies for CHRI Access, Use, Handling and Dissemination</b>	<b>86</b>
<b>Appendix G</b>	<b>LASO Responsibilities Handout</b>	<b>127</b>
<b>Appendix H</b>	<b>Sample Noncriminal Justice Agency Information Change Form</b>	<b>128</b>
<b>Appendix I</b>	<b>Sample Authorized Personnel List</b>	<b>129</b>

<b>Appendix J</b>	<b>Sample Training Documentation Form</b>	<b>130</b>
<b>Appendix K</b>	<b>NIGC Fingerprint MOU/CJIS Checklist and IT Security Audit Checklist</b>	<b>131</b>
<b>Appendix L</b>	<b>Key Employee and Primary Management Official Checklist</b>	<b>155</b>
<b>Appendix M</b>	<b>Bulletin – Fingerprint processing – Applicant Privacy Act rights and protecting CHRI</b>	<b>159</b>
<b>Appendix N</b>	<b>Sample Notice of Results</b>	<b>163</b>

## Introduction

The purpose of this guide is to assist federally recognized gaming tribes and their tribal gaming regulatory authorities (TGRA) in successfully submitting fingerprints to the National Indian Gaming Commission (NIGC). Pursuant to the Indian Gaming Regulatory Act (IGRA) and NIGC regulations, the NIGC processes fingerprints for persons at the tribes' gaming enterprises who come within the statutory and regulatory definitions of key employees and primary management officials. From the NIGC, tribes receive criminal justice information (CJI) and criminal history record information (CHRI) for noncriminal justice purposes pursuant to authorizations under federal law.<sup>1</sup> CJI refers 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. CHRI means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. CHRI is also information transferred or reproduced directly from CHRI, information that confirms the existence/ nonexistence of CHRI, letters, emails, documents, notes, conversations in person/phone, and databases including spreadsheets or tables.

Public Law 92-544, passed by Congress in October 1972, authorizes the FBI to exchange CHRI with officials of governmental agencies for noncriminal justice purposes (i.e., for licensing and employment). In 1998, the National Crime Prevention and Privacy Compact Act was passed allowing signatory states to exchange criminal history records for noncriminal justice purposes according to a uniform standard. The 1998 act also established the National Crime Prevention and Privacy Compact Council to regulate and assist in maintaining a method of exchange of CHRI, which protects both public safety and individual privacy rights. The FBI Criminal Justice Information Services (CJIS) Division houses the largest repository of fingerprint criminal history records and is responsible for overseeing the exchange of such records. Federal laws, regulations, and policies govern the release of information exchanged through the FBI and require states to regulate access, use, quality, and dissemination of state-held records.

Both state and federal criminal justice and CHRI is subject to laws, rules, and regulations governing its access, use, handling, and dissemination. This guide assists tribes and their noncriminal justice agencies with proper fingerprint submittals, provides guidance regarding agencies' responsibilities for appropriate information handling, informs agencies of requirements associated with the use of the state and federal criminal history check processes, as well as training offered by the NIGC. Additionally, it discusses the two sets of rules you will hear often is National Identity Systems requirements and CJIS Security Policy.

---

<sup>1</sup> 25 U.S.C. §§ 2706(b)(3), 2706(b)(7), 2706(b) (10), 2708, 2710(b)(2)(F), 2710(c)(1)-(2), 2710(d)(9), 2711(a), 2711(e), and 28 U.S.C. § 534.

## National Indian Gaming Commission Contact List

### Fingerprint Assistance

#### **NIGC Investigative Programs Specialist**

Available Monday through Friday from 8 a.m. to 5 p.m. Closed on Federal Holidays.

#### **NIGC Investigative Programs Specialist – Mr. Seneca Chavis**

Email: [fingerprint\\_admin@nigc.gov](mailto:fingerprint_admin@nigc.gov)

Phone: (202) 632-7003

Fax: (202) 632-7066

#### **Physical Address:**

National Indian Gaming Commission  
90 K Street NE, Suite 200  
Washington, DC 20002

#### **Mailing Address:**

National Indian Gaming Commission  
1849 C Street NW  
Mail Stop #1621  
Washington, DC 20240

### Technical Assistance

#### **National Indian Gaming Commission Technical Support**

Available Monday through Friday from 8 a.m. to 5 p.m. Closed on Federal Holidays.

#### **NIGC Information Security Officer**

Email: [iso@nigc.gov](mailto:iso@nigc.gov)

Phone: 202-632-7003

#### **Fingerprint Billing/Invoices**

Email: [Fingerprint\\_Billing@nigc.gov](mailto:Fingerprint_Billing@nigc.gov)

Phone: 202-632-7003

## Section 1 – General Overview

### 1.1 NIGC Overview

The NIGC is the Central Terminal Agency (CTA) for over 240 federally recognized tribes and their tribal gaming regulatory authorities (TGRA) for purposes of processing their key employee and primary management official applicants' electronic and ten print fingerprint cards through the FBI's IAFIS (Integrated Automated Fingerprint Identification System). The vast majority of the NIGC applicant cards are processed electronically through a NIGC-approved live scan vendor. Tribes without live scan equipment can mail ten print fingerprint cards (AKA hard cards) to the NIGC where the cards are scanned and submitted to the FBI electronically. The FBI then returns the results to NIGC to be shared with the tribe's TGRA for the sole purpose of determining the eligibility of applicants for key employee and primary management official positions in its gaming enterprise(s).

The NIGC system is designed so the NIGC and tribes do not use "FBI-approved Channelers". Channelers push and pull both CHRI and personally identifiable information (PII)/fingerprints. The NIGC and tribes use "NIGC approved live scan vendors" to simply push PII/fingerprints to NIGC and the NIGC pushes the CHRI data it receives from the FBI to the tribes. Some of the NIGC approved live scan vendors are also FBI-approved Channelers, but it is not a requirement. There is sometimes confusion about the two designations. For a list of NIGC approved live scan vendors please visit <https://www.nigc.gov/finance/fingerprint-process>. If you do not find your vendor on the list, please contact the NIGC Investigative Programs Specialist at [fingerprint\\_admin@nigc.gov](mailto:fingerprint_admin@nigc.gov) to confirm their status.

Under the CJIS Security Policy, the NIGC is required to designate a CJIS Systems Officer (CSO) to ensure that CHRI data is handled and stored properly at NIGC and at the tribes' locations. The CSO responsibilities include:

- Monitoring the NIGC and TGRAs' locations and systems to ensure system maintenance and records security, and
- Ensuring proper dissemination of CJI, including CHRI.

Established policies, procedures, and standards must be strictly adhered to in order to maintain the integrity of the system and its records. With respect to compliance with the federal regulations for system access and maintenance, the NIGC performs several duties:

- Conducting audits of the use and dissemination of CHRI and criminal history records,
- Training concerning use of system information, and
- Monitoring system access and researching/investigating security breaches.

### 1.2 Memorandum of Understanding

As the Central Terminal Agency (CTA) between the FBI and the Tribes, the NIGC entered into an updated Memorandum of Understanding (MOU) with the FBI on January 17, 2020. The MOU documents the agreed-upon responsibilities and function of the FBI and NIGC with respect to the submission of noncriminal fingerprints for primary management officials and key employees of Indian gaming enterprises, as defined by NIGC regulations, 25 C.F.R. §§ 502.14 (a-c) and 502.19 (a-c). For more information, see the NIGC and FBI MOU in Appendix A and Section 5.2 which covers the definitions of gaming operation, key employee and primary management official.

Each Tribe authorized to receive CJI and CHRI must sign a MOU with the NIGC. The MOU is a contractual agreement between the Tribe and NIGC. It must be signed by both an NIGC representative and the appropriate tribal official.

A sample of the current NIGC/Tribal MOU can be found in Appendix A. NIGC is developing a new NIGC/Tribal MOU in 2020 that all tribes must sign on or before January 1, 2021. The new NIGC/Tribal MOU will contain the following terms and conditions:

- Authority and Purpose: The MOU states the nature of the requesting organization, the purpose for which CJI and/or CHRI is requested, and the specific authorization granting access to the information. **It is prohibited for noncriminal justice agencies to use CJI and CHRI for any purpose other than that for which it was requested.**
- Sanctions/Penalties: The NIGC agrees to promptly notify tribal authorities if it determines that it is necessary to discontinue disseminating CHRI to the tribe (either in whole or in part) due to the tribe's failure to comply with conditions set forth in the MOU.
- Local Agency Security Officer: The new MOU requires the appointment of a Local Agency Security Officer (LASO) to act as liaison with the NIGC. (Section 4 of this guide covers the responsibilities of the LASO).
- Training: TGRAs are responsible for mandatory training requirements. TGRAs opening a fingerprint access for the first time must complete the Initial Access & NCJA Compliance Training prior to submitting fingerprint cards. For existing TGRAs, all tribal personnel who view or handle CHRI must complete the standard online training (currently called CJIS Online) and undergo tribal internal training on CHRI security and handling based on the required policies/procedures.
- Policies/Procedures: As part of privacy and security, TGRAs must implement policies and procedures that provide for the security and proper handling of the CJI/CHRI. TGRAs must also have rules for fingerprint submissions that include proper applicant identification and protecting fingerprint cards from tampering.

### 1.3 Authorizations and Access

Before access to the fingerprint system may be granted to a tribe, the tribe must contact the NIGC and request a pre-activation package. The packet includes a cover letter, systems requirements and a system checklist.

#### 1.3.1 Application for Access

Prior to submitting fingerprint cards and receiving CHRI, a tribe must complete a pre-activation packet, sign the NIGC/Tribal MOU and complete Initial Access & NCJA Compliance Training.

The training is designed to assist the tribe in carrying out its responsibilities under the MOU and maintaining compliance with laws and regulations. Once initial requirements are met, the NIGC will schedule activation and testing and the tribe is issued an Originating Case Agency number (OCA), which is a nine-character alphanumeric identifier. This number is the tribe's submission access number for fingerprint criminal history record checks. All submissions are made under the NIGC's ORI number which will be provided upon activation.

#### 1.3.2 Noncriminal Justice Access

Use of CHRI obtained from noncriminal justice fingerprints is strictly limited to the noncriminal justice purpose (licensing or employment) and **may not** be shared for criminal justice or any other purposes. Do not disseminate any forms of CHRI to anyone or any entity not directly involved in the licensing process at the Tribe and NIGC. The Tribe cannot duplicate, disseminate, or re-use CHRI, including sharing it with applicant's spouse, household, other family members, tribal leadership, other tribal agencies not involved in licensing key employees or primary management officials, human resource departments, other potential employers, and state gaming or licensing agencies. To be clear, even if the use of CHRI may be necessary to satisfy state licensing requirements, CHRI from NIGC cannot be used for such purpose – a new record request

to the FBI through a non-NIGC process must be made in such instances.

## **1.4 Outsourcing Agreements**

In accordance with the National Crime Prevention and Privacy Compact (Compact) Council's Final Rule entitled "Outsourcing of Noncriminal Justice Administrative Functions" (28 C.F.R. part 906), outsourcing of noncriminal justice administrative functions is permitted under certain conditions when approved by the FBI Compact Officer and as specified in the Security and Management Control Outsourcing Standard for Non-Channelers (Outsourcing Standard) located at <https://www.nigc.gov/compliance/CJIS-Training-Materials>.

### **1.4.1 Outsourcing Agreement Submission**

Non-channeler Outsourcing Agreements are required when a TGRA uses an entity, contractor or vendor to assist it with handling, storing, or moving electronic or physical CJI or CHRI. To ensure compliance with the standard, if the TGRA uses a third party, including the casino's or tribe's Information Technology (IT) department, to maintain the network, servers or computers which access and store CHRI, an outsourcing agreement must be drafted and submitted to the FBI Compact Officer for approval prior to executing the agreement and engaging the service.

To contract noncriminal justice administrative functions to a third party, the TGRA must submit a letter requesting approval to use the entity, contractor, or vendor to the FBI Compact Officer, copying the NIGC CSO at [iso@nigc.gov](mailto:iso@nigc.gov). The letter is standard format and a sample can be found in Appendix B.

Additionally, a draft, unexecuted contract between the TGRA and the contractor must accompany the request letter. A sample contract can be found in Appendix B.

### **1.4.2 Contract Regarding Outsourcing Noncriminal Justice Functions**

The contract is standard format and details the parties, what functions are to be outsourced, and the requirement for all CJI and personal identifying information (PII) to be returned to the tribe upon termination of the contract. Upon receiving approval from the FBI Compact Officer, the TGRA and contractor can execute the approved draft contract. Additionally, the TGRA must audit the contract and contractor within 90 days of its execution and certify compliance to the FBI Compact Officer. A sample audit can be found in Appendix B.

#### **Examples of when Outsourcing Agreements are needed:**

**Shredding:** If a TGRA wants to employ a shredding company to destroy CHRI and/or summary CHRI at the TGRA location or are allowed to leave with the documents, an approved outsourcing contract is required.

**Storage:** If the Tribe uses an off-site storage facility for document storage including CHRI or summary CHRI and storage facility employees have access to CHRI in the box or the facility employees store the CHRI in a locked container that they control, an outsourcing contract is required.

**Public Telecom Carriers:** If the Tribe uses a public telecom service, which has access to servers,

or provide patches to the servers where CHRI is stored, an outsourcing contract is required. If the telecom service does not have access to the servers or provide patches, outsourcing is not required, which is typically the case.

**Electronic Media:** If a third party stores electronic CHRI data for a tribe an outsourcing contract is required.

**Live Scan Vendors :** If a NIGC-approved live scan vendor solely provides live scan service to the TGRA and does not have access to CHRI, an outsourcing contract is not needed. However, if the live scan vendor has access to CHRI<sup>2</sup> or provides services over and above live scan activities, including but not limited to - data storage of CHRI, network maintenance, or licensing applications where CHRI is stored or summary CHRI information is documented - an outsourcing agreement is required.

If the tribe receives and/or stores CHRI results on the same laptop or computer the live scan device is uses to send the fingerprints to NIGC and the live scan vender has, at any point in time, access, escorted or unescorted, to the CHRI information, an outsourcing agreement is required.

If the tribe purchased the laptop from the live scan vender and has a service agreement for the laptop where CHRI results are received and/or stored, an outsourcing agreement is required.

In summary, if any entity, contractor, or vendor has access to electronic summary CHRI data in electronic or hard-copy form, an outsourcing contract is required.

---

<sup>2</sup> This includes any indication that a FBI CHRI record exists or does not exist for a given applicant.

## Section 2 - Fingerprint Submissions & Results

The information in this section is intended to assist tribes with the following:

- Understanding the fingerprinting process with the NIGC
- Applicant identity verification and fingerprint card tampering prevention
- Complying with FBI applicant privacy notification requirements
- Filling out the fingerprint card properly
- Assembling a fingerprint submission packet
- Interpreting FBI results

### 2.1 NIGC Fingerprinting Process

There are two fingerprinting processes to obtain CHRI results through the NIGC—electronic fingerprint and hard card fingerprint submissions. The subsections below explain the fingerprint criminal history check process. Please note that this guide concentrates on electronic fingerprint submissions and compliance rules for the fingerprint criminal history check process.

#### 2.1.1 Fingerprint Criminal History Check Process

In the fingerprint criminal history check process, the tribe has a legal authorization via IGRA and NIGC regulations to submit applicant fingerprints to the NIGC. The process takes place between the tribe and the NIGC whereby the tribe submits the prints and the available criminal history record is sent to the tribe for review. If there is no criminal history, the NIGC and/or FBI results report will indicate a negative response. The use of the criminal history results is limited for the sole purpose outlined in IGRA – employment and/or licensing of key employees or primary management officials in the tribe’s gaming enterprise. The Tribe must have an active MOU on file with the NIGC and is subject to compliance regulations and periodic audits.

The fingerprint criminal history check process is a “point in time” check, and a tribe may only see changes to a person’s criminal history if the fingerprints were submitted again. With a fingerprint criminal history check, the tribe sees the actual criminal history and makes the eligibility determination regarding the applicant, not the NIGC. The NIGC may object to the licensing of an applicant based on criminal history or other background investigation findings; however, the final licensing decision is made by the tribe.

### 2.2 Applicant Identification

Agencies must have quality assurance processes for verifying the identity of the applicant at the time of fingerprinting.

The National Crime Prevention and Privacy Compact Council published the *Identity Verification Program Guide* containing suggestions and best practice recommendations for verifying an applicant's identity and safeguarding the integrity of the fingerprints. A copy of the guide can be downloaded from the FBI website in the Compact Council section at <https://www.fbi.gov/services/cjis/compact-council>. Compact Council recommendations regarding proper identification of applicants include:

Accept only valid, unexpired photo identification documents as primary proof of identity.

- When accepting secondary identification (i.e. birth certificate, Social Security card), ask for supporting documentation such as a utility bill, bank statement, or mortgage documents.
- Use additional identification data support methods such as:
  - Examine the applicant’s photograph on the identification provided and visually compare the picture with the applicant.

- Compare the physical description on the documentation to the applicant's features (e.g. height, weight, hair and eye color, age, etc.)
- Request the applicant to verbally provide date of birth, address, etc. and verify the answers with the identification provided.
- Check the applicant's signature provided in person with a signature on the identification provided.
- Examine the provided identification to ensure that it has not been altered in any manner.

### **2.3 FBI Applicant Privacy Rights Notice and FBI Privacy Act**

Per Title 28 C.F.R. 50.12 (b), whenever a tribe submits fingerprints for FBI criminal history record checks, the following actions/disclosures are required:

- The person being fingerprinted, meaning the applicant, must be:
  - provided a written FBI Privacy Act Statement (dated 2013 or later) when submitting their fingerprints and associated personal information; and
  - notified in writing that the fingerprints will be used to check the criminal history records of the FBI.
- Simply stating that the applicant is subject to a “national background check” is NOT sufficient.
- The applicant must be informed that they are allowed a reasonable time to change, correct, update, complete, and/or challenge the accuracy of their criminal history record. ALL applicants must be advised of this right, not just those who dispute an employment/license denial.
- The applicant must be advised about how to obtain a copy of their FBI criminal history record and the procedures for challenging it or obtaining a change, correction, or update to it as set forth in Title 28 C.F.R. § 16.34. The tribe may provide a copy of the record to the applicant for this purpose, if it has established a written policy to do so.
- The tribe must also establish and document what constitutes a reasonable period of time for a review and challenge to a record and any appeals process that is available to an applicant for such a challenge.
- If the applicant elects to review/challenge the criminal history record, the tribe must provide the applicant a reasonable period of time to do so before making licensing or employment decision.

A copy of the *Noncriminal Justice Applicant's Privacy Rights* and the *FBI Privacy Act Statement* can be found in Appendix C of this guide and at the NIGC website at <https://www.nigc.gov/compliance/CJIS-Training-Materials>. The FBI updates the notices periodically (usually in the June or November), so the Tribe is encouraged to visit the FBI CJIS websites often to ensure current documents are used:

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

<https://www.fbi.gov/services/cjis/compact-council/guiding-principles-noncriminal-justice-applicants-privacy-rights>

### **2.4 Electronic (Live Scan) Fingerprint Submission System Connectivity**

The NIGC, using an AltaScan Store and Forward (SnF) system and a Post Office Protocol 3 (POP3) mail server, provides each tribe a network connectivity path to the FBI's IAFIS system. The SnF is capable of receiving ANSI NIST/EFTS 6.2 and EFTS 7.0 compliant submissions for processing to the IAFIS. Additionally, the SnF is capable of receiving electronic FBI results (SRE) and CHRI as well as Ten Print Transaction Errors (ERRT) and returning these to the submitting tribe. The NIGC interface provides an industry standard, open connectivity path for any tribe, using any EFTS compliant system, to connect and submit electronic fingerprint submissions for processing by the FBI. To ensure convenient and open connectivity, the NIGC choose to use the Internet to allow agencies to transmit and receive fingerprint transactions. Therefore, each tribe will need an Internet Service Provider (ISP) to allow their fingerprint submission system (or device) to access the Internet. Because the fingerprint submissions are rather large files (350 Kb to 1 Mb), NIGC recommends the connection speed be at least 56Kbs to maximize submission throughput. Each tribe should scale the provided bandwidth to accommodate expected fingerprint activity.

If a tribe has a firewall, ports 500 and 4500 will need to be open for two-way traffic.

The tribe's fingerprint system must use a strong authentication and encryption process to submit fingerprints electronically. The fingerprint system should also be configured to register for and use group authentication.

The Tribe's fingerprint system should be configured to send the electronic submissions to the NIGC provided Fingerprint Internet Mail Server (SMTP). The 'To' address is provided on the Pre-Activation checklist for initial set up.

The SnF will process the submissions and receive the FBI results. The SnF will then send the FBI result to the tribe's mailbox located on the NIGC Fingerprint Internet Mail Server (POP3). The tribe's fingerprint system should be configured to retrieve their fingerprint results from this mailbox. The FBI's return policy for applicant submissions is 24 hours. However, most responses usually arrive between 20 minutes and 1 day after submission. The Fingerprint Internet Mail Server holds the responses in the mailbox until the tribe connects and retrieves them. The SnF system will also send a copy of the FBI results to the tribe's designated NIGC regional office.

The tribe's fingerprint system should be configured to limit the amount of times VPN connections can be made to the NIGC's VPN in order to retrieve FBI results. The NIGC's VPN gateway services the tribe's access to the NIGC Fingerprint system as well as remote access for NIGC offices and personnel. To ensure all users will have reasonable access to retrieve FBI results in a timely manner and that the VPN gateway resources are not over utilized, the Tribe's fingerprint system should be configured to access the VPN gateway at no less than 15 minute intervals.

For more information on System Security, System Protocols and Data Requirements please see Appendix D.

## **2.5 Mail Reply(s):**

After submissions are successfully sent to the FBI's IAFIS system, results are returned electronically to the NIGC's AltaScan SnF, which, in turn, sends the results to the NIGC Fingerprint Internet Mail Server (POP3) and ultimately to the submitting tribe. In order to correctly send responses back to the submitter, all electronic submissions should have a tribe specific, NIGC issued, return e-mail address in the "from" line of the submission. The NIGC's SnF system dynamically links the "From" address of a submission to the TCN/TCR number(s) of each submission. This allows the submitter end to change without re-configuring the NIGC's systems. Again, the "From" line of the submission is provided in the Pre-Activation Checklist.

The submitting device must be capable of accepting ANSI NIST/EFTS compliant responses as reply messages. These messages must be de-MIME'd and interpreted by the submitter when received. The responses will provide Ident and Non-Ident information. For Ident responses, the FBI will attach the RAP sheet if requested and is available. In order to receive RAP sheets, the submission must have Request for Rap Sheet (2.070) set to 'Y' for Yes.

## **2.6 System Testing:**

Submission testing must be completed before any electronic submitter can go "live." The tribe will send an email to [Itsupport@nigc.gov](mailto:Itsupport@nigc.gov) in order to request for a time slot to conduct a test. One of the Itsupport personnel will coordinate the testing date and the account will be converted into a test mode in the NIGC fingerprint system. As soon as the account is in test mode, the tribe submits or transmits a test electronic fingerprint data with a SSN starting with 002-00-0001. The tribe should receive a response from the FBI by logging in into the NIGC fingerprint system. Upon successful completion of the test, the tribe will send an email to [Itsupport@nigc.gov](mailto:Itsupport@nigc.gov) requesting that the account will be converted into a production mode.

## 2.7 Step by Step Transaction flow(s):

After complying with the above sections, a request by the authorized tribal personnel should be submitted to [itsupport@nigc.gov](mailto:itsupport@nigc.gov) for the following: a) Connection parameters to the NIGC fingerprint system ; b) Instructions on the VPN client to install for Windows 10 only; c) If utilizing the Cisco 5.x client, please consult with your fingerprint vendor to obtain the Cisco 5.x client.

The following is a step-by-step transaction flow of a typical submission:

1. An applicant's fingerprint images are scanned by a Scan device (Live Scan or Card Scan) and formatted into an EFTS compliant electronic NIST record. All applicable demographic information is entered and automatically attached (single part) to the ten print scan. The scanner device will format the images and demographics into an EFTS compliant submission. (See your scan device documentation for details).
2. The tribe's submission device will connect to the Internet. The bandwidth of the connection should be sized according to the expected volume bearing in mind that each NIST submission will range in size from 350Kb to 1 Mb. The NIGC recommends at least a 56 Kbps modem connection.
3. Once a connection to the Internet is established, an IPSec connection or L2PT connection to the NIGC firewall (VPN gateway) will be initiated. The firewall will authenticate the group authentication name and password. If the group authentication settings are valid, the IPSec connection is established.
4. The Live Scan or Card Scan device will then Email the NIST submission DIRECTLY to the NIGC Fingerprint Internet Mail server using (SMTP) and it should be addressed to an address provided by the NIGC (normally [triberelay@NIGCEXT01.NIGC.GOV](mailto:triberelay@NIGCEXT01.NIGC.GOV)). In turn, the NIGC Fingerprint Internet Mail server will be forwarded to the NIGC's SnF server. We do not allow split tunneling or routing the submission to an outside server before being sent to NIGC Fingerprint Internet Mail server.
5. The SnF server will parse the submission, retaining all information in the SnF database and perform various data analysis (edit checks) to ensure a proper submission. During the edit checks, the SnF will match the OCA field (2.009) to the sender's address to ensure proper accounting and billing. If the SnF server finds an error that prevents processing the submission, the SnF will return an electronic response, similar to the FBI's ERRT (see step 11) and the submission will not be sent to the FBI. After correcting the problem, the tribe should create a new submission (new TCN) and transmit. The tribe will not be charged for the submissions that the SnF rejects.
6. After the submission is processed, the NIGC's SnF server will send the submission to the FBI's IAFIS for processing.
7. The FBI's IAFIS takes anywhere from 20 minutes to 24 hours to process the submission and send a response. The average is 2-3 hours. Once they have completed processing, the FBI will send a response containing either a "no record found" called a Nonident or an Ident. The FBI Rap sheet will be attached if the "Request for Rap Sheet" field (2.070) is set to "Y" for Yes. If this field is missing or set to 'N' for No, the submitter will only receive the Ident record. If you do not receive a response from the NIGC after 24 hours, please contact the NIGC Fingerprint Administrator.
8. The NIGC's SnF server will parse the response, retain all the necessary information in the SnF database and return the response to the tribe's mailbox on NIGC Fingerprint Internet Mail server. The SnF uses the 'From' address of the corresponding submission.

9. The NIGC Fingerprint Internet Mail server will queue the response in the previously associated POP3 account and hold the response until retrieved by the tribe's scan device.
10. The tribe's system will initiate a second IPSec tunnel or L2TP tunnel and connect to their POP3 account to retrieve the queued responses. Submitting systems should be configured to connect no more frequently than once every fifteen minutes to retrieve responses.
11. If the submission has an error or the image quality of the fingerprint images is corrupted or unreadable, the FBI will return a Ten Print Error Transaction (ERRT). This error response lists the problems that occurred in the invalid fields or will describe the image quality problems. This ERRT will be processed and emailed to the submitting tribe and NIGC regional office (See next step).
12. The ERRT will contain the FBI TCN (Transaction Control Reference). This number is quickly identified because it begins with FBI TCN: E200 and is 20 characters long. When the tribe fixes the problem that caused the error, a new submission must be submitted (new TCN (TCR)) and the FBI TCN (Transaction Control Reference) is entered in the TCR (1.10) tag field. This allows the tribe to resubmit the transaction without being billed again.

## **2.8 Basic Hard Card Fingerprinting Tips**

There is no certification requirement with the NIGC to be able to take fingerprints. The only requirement is developing a proficient technique for taking clear, clean fingerprints. The tips here should help you get started, and then all you need is practice.

## **Basic Fingerprinting Tips**

### **Fill out the top of the fingerprint card first.**

All the applicant's information should be on the card and the applicant should sign the card prior to taking the prints. This will avoid accidentally smudging the prints.

### **Have the applicant wash their hands.**

Dirt or other particles on the fingers can obscure characteristics, cause smearing, and create inaccurate marks in the print. If the applicant has excessive perspiration on the hands, wipe each finger with a cloth before inking and then roll the print immediately. Using rubbing alcohol and letting it dry can also temporarily dry the skin enough to allow printing. (If using a live scan instrument, be sure that the fingerprint plate is clean and free of oils, dust, and residue from previous prints before beginning.)

### **Use only heavy black ink intended for fingerprinting.**

Other types of ink smear or do not provide adequate coverage. "Inkless" fingerprint pads do not provide acceptable prints.

### **Use the right amount of ink.**

Not fully inking the finger prior to rolling can result in "gaps" and missing characteristics in the prints. Too much ink can cause heavy smears or obscure the ridges of the print. Too little ink may result in impressions that are too faint. Fingerprints should be dark gray for best results.

### **Control the person's hand.**

Ask the applicant to relax and let you do the work. Asking them to look away from the card may prevent them from unconsciously "helping", which may cause twisting or slipping while trying to roll the finger.

### **Use the "awkward to easy" roll method.**

The boxes on the fingerprint card marked for individual fingers must be rolled fingerprints. Rolled prints are made by rolling the finger or thumb from nail edge to nail edge. The fingerprint should show the surface of the fingerprint from fingertip to just past the first joint on the finger, and the entire print must fit within the blue lines of the box designated for that finger. Grasp the top of the applicant's hand and extend the finger to be printed. Roll in one continuous motion using only enough pressure to make a clear print with no "gaps" in the ink; too much pressure may smear the print. For best results, roll fingers on the right hand toward the right, and fingers on the left hand toward the left, going from "awkward" (where the hand/wrist is most uncomfortable) to "easy" (where the hand/wrist ends up in a comfortable natural position). This helps prevent the person resisting and making unexpected movements as you roll. Thumbs are rolled in the opposite direction than fingers on that hand. After reaching the end of the "roll", lift the finger straight up to avoid smearing or stray ink on the card.

### **Position the hand well for the "flat" prints.**

The bottom row of blocks on the fingerprint card is for pressed or "flat" (also known as "plain") impressions. Make sure all four fingers are extended straight and stiff from the hand. Position the hand at an approximately 45 degree angle to the card to ensure that all four fingers will fit into the box. Print as much of the fingers as you can fit, but at least to just past the first joint. Print all four fingers at the same time by pressing down; no "rolling".

Press down slightly on the top of the applicant's fingers to ensure a complete print with no "gaps" and then lift straight up. Thumbs are pressed straight down into the designated block next to the finger impressions. Use care not to overlap the prints or the lines of the boxes.

### **Use careful technique for "worn" fingerprints.**

Some applicants may have "worn" fingerprints with thin or faint ridges. Use less ink, not more, and light pressure to achieve the best results. Squeezing the finger or "milking" it by rubbing down along the length of the finger toward the tip may help raise the ridges.

If you are going to fingerprint on-site at your tribe, then you will need to obtain black fingerprinting ink. Inkless, gel, and watermark ink do not yield acceptable fingerprints. The NIGC does not provide fingerprinting ink.

## 2.9 Protection of the Fingerprint Card Prior to Submission

TGRAs must have quality assurance processes for protecting the integrity of the fingerprint card and preventing tampering with the card from the time the prints are taken through the submission process.

Suggestions and recommendations for tampering prevention processes can be found in the National Crime Prevention and Privacy Compact Council's *Identity Verification Program Guide* located at <https://www.fbi.gov/services/cjis/compact-council>. Recommendations include:

- Implement forms to standardize the information gathered with each applicant and document the type of photo identification presented by the applicant.
- Establish procedures that use specially sealed envelopes, tribe specific stamps, etc. for the tribe to use as part of a chain-of-custody process for manually captured fingerprints.

## 2.10 Required Information for Each Fingerprint Card Submission

The following information is intended to assist tribal personnel in ensuring that the blocks on the fingerprint card are properly completed. Either tribal personnel or the applicant can fill out the card, but it is the tribe's responsibility to review the information on the card for accuracy and completion, and verify the applicant's identity. If the tribe fills out the card, the applicant should review the card for accuracy before signing it. Errors, missing information, and information placed in the wrong areas can all cause delays in processing. Please type or print legibly in black ink.

### 2.10.1 Fingerprint Card Legend

1. **Applicant's full name:** The name should be in the last name, first name, middle name sequence.
2. **Signature:** This is the applicant's signature. Please ensure that the applicant has signed the card in INK.
3. **Residence Address:** This is the applicant's physical residential address, NOT the mailing address.
4. **Aliases (AKA):** Enter any known aliases, including maiden names.
5. **ORI:** Only fingerprint cards indicating the National Indian Gaming Commission (USNIGC00Z) may be used. The block should be preprinted with "USNIGC00Z – Natl Ind Gaming Comm, Washington, DC".
6. **Date of birth (DOB):** The date of birth should be in MM/DD/YYYY format.
7. **Date:** This is the date the applicant was fingerprinted.
8. **Signature of Official Taking Prints:** The signature of the person at the tribe or office taking the prints should be placed in this box.
9. **Your No. OCA:** The submitting tribe's OCA should be written here. This alphanumeric identifier is nine characters long.

10. **Sex:** **M** for Male, **F** for Female

11. **Race:** Enter the one letter abbreviation for race.

**A** Asian/Pacific Islander

**B** Black

**I** American Indian or  
Alaskan Native

**W** White or Hispanic

**U** Unknown

12. **Height:** Enter the height in feet and inches. Example: An applicant who is 5 feet 7 inches tall should be entered as 507, not 67 inches. An applicant who is 5 feet 10 inches tall should be entered as 510.

13. **Weight:** Enter the weight in pounds as a whole number. Numbers under 100 should be entered as three numbers with a leading zero. Example: 95 pounds should be entered as 095.

14. **Eye & Hair Color:** Enter the three letter abbreviation for the applicant's eye and hair color.

**EYE COLOR**

**BLK** Black

**BLU** Blue

**BRO** Brown

**GRN** Green

**GRY** Gray

**HAZ** Hazel

**MAR** Maroon

**MUL** Multicolored

**PNK** Pink

**HAIR COLOR**

**BLK** Black

**BLN** Blond or Strawberry

**BLU** Blue

**BRO** Brown

**GRN** Green

**GRY** Gray or Partially Gray

**ONG** Orange

**PLE** Purple

**PNK** Pink

**RED** Red or Auburn

**SDY** Sandy

**WHI** White

**XXX** Unknown or Completely  
Bald

15. **Place of birth:** If born in the United States, enter the two letter state abbreviation (e.g., AZ). If the place of birth is a foreign country, enter the full name of the country (do not abbreviate).

16. **Employer and Address:** Enter the name and address of the tribe that is submitting the fingerprint card. This tribe must be the same tribe that is assigned to the OCA written in the “Your No. OCA” block.
17. **Reason fingerprinted:** Enter “Indian Gaming Licensee”.
18. **Social Security Number:** Enter the social security number of the applicant in XXX - XX - XXXX format. If the applicant does not have a social security number, leave this blank.
19. **Rolled prints in proper box for each finger:**
- A complete set of inked fingerprint impressions must be submitted.
  - Fingerprints must be rolled from side of nail to side of nail. All impressions must be within the correct blue box for that print with no overlapping.
  - All impressions should be taken in proper order. The prints must be legible and classifiable.
  - If a finger cannot be printed, indicate a reason in the correct finger block:
    - For a finger that was physically severed and is missing the first joint or more, you may enter "AMP" in the correct box for that finger. If the finger has been physically missing the first joint or more since birth, it is also acceptable to write "missing since birth".
    - If a portion of the first joint is still present ("tip amputated"), print the available fingerprint remainder as you normally would. If a finger is present but severely scarred, print it as you normally would.
    - Attempt to fingerprint deformed fingers; use a notation only if attempts to print have failed. If the finger cannot be printed due to injury (such as a broken bandaged finger) or severe deformation, indicate the reason for the missing print in the correct fingerprint box (e.g., "bandaged", "injured", "paralyzed").
  - See the reverse side of the card for information regarding requirements in taking a good set of fingerprints. The FBI website at [www.fbi.gov](http://www.fbi.gov) offers tips for taking proper legible fingerprints. Type *Recording Legible Fingerprints* and *Capturing Legible Fingerprints* in the website search box to find these tips.
  - If a rolled print is smeared or otherwise unacceptable, you may cover it with an adhesive tab and try again. No more than two retabs may be used on a single fingerprint block.
20. **Pressed simultaneous prints in proper boxes:** Do not roll fingerprints in these boxes: these are known as "flat" or "slap" prints. Fingers are pressed down together and then lifted straight up. Thumbs are pressed down separately in the appropriate box. Ensure prints are placed in the proper boxes with no overlapping. Do not overlap the blue lines of the box.

## 2.11 Example Fingerprint Card

<b>APPLICANT</b>		LEAVE BLANK		TYPE OR PRINT ALL INFORMATION IN BLACK				FBI		LEAVE BLANK	
SIGNATURE OF PERSON FINGERPRINTED		LAST NAME <u>NAM</u>		FIRST NAME		MIDDLE NAME					
SIGNATURE OF APPLICANT		OTHER NAMES		OR		USNIGC00Z					
RESIDENCE OF PERSON FINGERPRINTED		INCLUDING MAIDEN		CITIZENSHIP <u>CTZ</u>		DATE OF BIRTH <u>DOB</u>		MM/DD/YYYY		PLACE OF BIRTH <u>POB</u>	
STREET ADDRESS		YOUR NO. <u>OCA</u>		SEX <u>SEX</u>		RACE <u>RACE</u>		HGT <u>HGT</u>		WGT <u>WGT</u>	
CITY, STATE, ZIP		YOUR TRIBE'S OCA		ARMED FORCES NO. <u>MNU</u>		EYES <u>EYES</u>		HAIR <u>HAIR</u>		STATE	
DATE		FINGERPRINT TECH NAME/ID #		SOCIAL SECURITY NO. <u>SOC</u>		SOCIAL SECURITY #		CLASS		REF.	
EMPLOYER AND ADDRESS		NAME OF TRIBE		MAILING ADDRESS		CITY, STATE ZIP		INDIAN GAMING LICENSEE			
<b>→ ROLL PRINTS</b>											
Right thumb		Right index finger		Right middle finger		Right ring finger		Right little finger			
1. R. THUMB		2. R. INDEX		3. R. MIDDLE		4. R. RING		5. R. LITTLE			
<b>→ ROLL PRINTS</b>											
Left thumb		Left index finger		Left middle finger		Left ring finger		Left little finger			
6. L. THUMB		7. L. INDEX		8. L. MIDDLE		9. L. RING		10. L. LITTLE			
<b>→ PRESS PRINTS FLAT</b>											
Left four fingers taken at the same time		Left thumb		Right thumb							
LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY		L. THUMB		R. THUMB		RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY					

## 2.12 Payment and Submission Packets

This subsection contains fee information and payment submittal requirements.

### 2.12.1 Fees

(Current fees as of November 1, 2019)

Current fee per fingerprint submission	\$22.00 per card
Resubmission due to rejection if using the Transaction Control Numbers	\$0 per card
Search requests if using the Transaction Control Numbers	\$0 per card request

### 2.12.2 Payment Submittal Requirements

Fingerprint statements are processed on a monthly basis and mailed to the tribe address and contact provided to the NIGC. Payments of fingerprint fees are due within 30 days of the fingerprint statement.

The NIGC DOES NOT accept personal checks, cash, or credit/debit cards.

Make the payment instrument payable to the **National Indian Gaming Commission**.

### 2.13 Rejected Fingerprint Cards/Resubmissions

When fingerprint submissions are rejected, you will receive a NIGC and/or an FBI notice with the reason for the rejection.

If cards are rejected for incomplete/inaccurate information, carefully follow the instructions on the reject notice.

If the fingerprint cards were rejected because the fingerprints are illegible or unclassifiable, a new fingerprint card will be needed. Always include a copy of the reject notice/FBI reject sheet with your resubmission

#### Example FBI Reject Sheet

<b>REJECT</b>
1.01: 158
1.02: 0201
1.03: 1
1.04: ERRT
1.05: 20021124
1.06: 4
1.07: WVIAFIS0Z
1.08: WVIAFIS0Z
1.09:
IFCS000X151902662170
1.10: 2A09000030
1.11: 00.00
1.12: 00.00
2.001: 466
2.060: L0008 - THE QUALITY OF THE CHARACTERISTICS IS TOO LOW TO BE USED. HOWEVER, POSSIBLE CANDIDATES WERE FOUND. PLEASE SUBMIT A NEW SET OF FINGERPRINTS FOR COMPARISON TO THE CANDIDATE(S).
<b>Reason for reject</b> ▲

Applicant cards rejected by the FBI for poor print quality can be resubmitted ONCE free of charge; however, the resubmitted card MUST be received by the FBI within one calendar year of the date of the original reject.

#### 2.13.1 Routine Name Search Procedure

A routine name search procedure requests the FBI to use the name, date of birth, and Social Security number of the applicant whose fingerprints have been rejected twice by the FBI to make a physical search and comparison of their fingerprints to any fingerprint records on file matching their personal information. A fingerprint expert will conduct an examination of the fingerprints and determine with a degree of certainty, if possible, that the prints the tribe submitted did or did not match the records on file at FBI. If they do match, the records on file will be reported to the NIGC and shared with the tribe.

The tribe must follow the routine name search procedure if the fingerprints are rejected twice because the fingerprints are illegible or unclassifiable by the automated process or if the tribe is required to present a page with the applicant's name on it to prove negative FBI name search results.

#### Routine Name Search Procedure

- 1) The fingerprints must have been rejected twice by the FBI.
  - a) The first reject must be within the past year.
  - b) The name search request must be submitted within 90 days following the second reject.
- 2) The tribe must complete and submit the CJIS Name Search Request Form located in Appendix D of this guide. The TCN is the number below the bar code on the fingerprint card. Enter the TCN of the last two fingerprint cards that were rejected by the FBI. Write your tribe's OCA in the OCA field. When the form is completed, FAX the form to the NIGC Systems Specialist. It takes two to three weeks to receive the results back from the FBI depending on their volume. The results will be forwarded to your Tribe.

If the FBI cannot process the request they will fax it back with a reject notice indicating why they could not complete the request.

A copy of the CJIS Name Search Request can be found in Appendix E.

#### **2.13.2 Example Individual FBI Reject Notice**

	<b>REJECT</b>
	1.01: 158
	1.02: 0201
	1.03: 1
(1)	1.04: ERRT
	1.05: 20021124
	1.06: 4
	1.07: WVIAFIS0Z
	1.08: WVIAFIS0Z
(2)	1.09: IFCS000X151902662170
(3)	1.10: 2A09123457
	1.11: 00.00
	1.12: 00.00
	2.001: 466
	2.002: 00
(4)	2.006: XX000000E
	2.007:
(5)	2.060: L0008 - THE QUALITY OF THE CHARACTERISTICS IS TOO LOW TO BE USED.
(6)	2.073: USNIGC00Z
	2.092:
	2.128:
	2.600:

#### **FBI Reject Notice Legend**

- (1) Error message

- (2) Information used by NIGC for resubmission
- (3) TCN assigned by NIGC
- (4) Submitting Tribe's OCA
- (5) Reject code and reason for reject
- (6) NIGC ORI

## **2.14 Example FBI Criminal History Record**

### **Federal Criminal History Record Legend**

- (1) Information used by NIGC for resubmission
- (2) PCN assigned by NIGC
- (3) Submitting Tribe's OCA
- (4) Subject's name
- (5) IDENT (indicates an FBI record)
- (6) NIGC's ORI
- (7) Subject's name
- (8) Subject's personal identifiers
- (9) Federal use and dissemination restrictions
- (10) Warrant notification
- (11) Warrant
- (12) Arrest information
- (13) Offenses/Charges
- (14) Information regarding disposition
- (15) Arrest information
  - Date of arrest or date fingerprint card received by FBI
- (16) Court information
  - Sentence (look for the disposition here for above arrest)
- (17) Arrest information (second arrest – different date and agency)
  - No court and no disposition noted in example
- (18) CRIMINAL HISTORY – Introduces criminal history record information from a state's criminal justice information system.
- (19) CYCLE – Some states use cycle numbers to separate arrest from one another.
- (20) ARRESTING AGENCY - Contains the arresting agency's name and ORI. The first two characters of the ORI are the state abbreviation.

(21) Some states also provide prosecution agency information.

**NOTE:**

The FBI criminal history record consists of different formats from each state's criminal justice information system. When reading the FBI criminal history record, look for key terms such as arrest, charge, count, court, disposition, level, sentence, severity, etc.

- 1.01:178
- 1.02:0500
- 1.03:11-200
- 1.04:SRE
- 1.05:20161118
- 1.06:4
- 1.07:USNIGC00Z
- 1.08:WVIAFIS0Z
- (1) 1.09:E20160000000000000000
- (2) 1.10:2A09123456
- 1.11:00.00
- 1.12:00.00
- 1.13:00.00
  
- 2.001:0000
- 2.002:00
- (3) 2.006:XX000000E
- 2.014:000000000
- (4) 2.018:SMITH, BRAD
- (5) 2.059:I
- (6) 2.073:USNIGC00Z

---

UNITED STATES DEPARTMENT OF JUSTICE  
 FEDERAL BUREAU OF INVESTIGATION  
 CRIMINAL JUSTICE INFORMATION SERVICES DIVISION  
 CLARKSBURG, WV 26306

USNIGC007Z  
 PCN 2A09123456

THE FBI IDENTIFIED YOUR TEN-PRINT SUBMISSION WHICH  
 CONTAINED THE FOLLOWING DESCRIPTORS:

- (7) NAME SMITH, BRAD
  
- (8)
 

SEX	RACE	BIRTH DATE	HEIGHT	WEIGHT	EYES	HAIR
M	W	1954/01/11	603	235	BROWN	BLACK

STATE ID	BIRTH PLACE
NULL	TEXAS

OTHER BIRTH DATES	SOCIAL SCARS-MARKS-TATTOOS	SECURITY	MISC NUMBERS
NONE	NONE	000-00-0000	NONE

  
 ALIAS NAME(S)  
 NONE  
  
 END OF COVER SHEET

UNITED STATES DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION  
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION  
CLARKSBURG, WV 26306

USNIGC007Z  
NCNE20160000000000000000

BECAUSE ADDITIONS OR DELETIONS MAY BE MADE AT ANY TIME, A NEW COPY SHOULD BE REQUESTED WHEN NEEDED FOR SUBSEQUENT USE.

THIS RECORD IS SUBJECT TO THE  
FOLLOWING USE AND DISSEMINATION RESTRICTIONS

(9) UNDER PROVISIONS SET FORTH IN TITLE 28, CODE OF FEDERAL REGULATIONS (CFR) SECTION 50.12, BOTH GOVERNMENTAL AND NONGOVERNMENTAL ENTITIES AUTHORIZED TO SUBMIT FINGERPRINTS AND RECEIVE FBI IDENTIFICATION RECORDS MUST NOTIFY THE INDIVIDUALS FINGERPRINTED THAT THE FINGERPRINTS WILL BE USED TO CHECK THE CRIMINAL HISTORY RECORDS OF THE FBI. IDENTIFICATION RECORDS OBTAINED FROM THE FBI MAY BE USED SOLELY FOR THE PURPOSE REQUESTED AND MAY NOT BE DISSEMINATED OUTSIDE THE RECEIVING DEPARTMENT, RELATED AGENCY OR OTHER AUTHORIZED ENTITY. IF THE INFORMATION ON THE RECORD IS USED TO DISQUALIFY AN APPLICANT, THE OFFICIAL MAKING DETERMINATION OF SUITABILITY FOR LICENSING OR EMPLOYMENT SHALL PROVIDE THE APPLICANT THE OPPORTUNITY TO COMPLETE, OR CHALLENGE THE ACCURACY OF, THE INFORMATION CONTAINED IN THE FBI IDENTIFICATION RECORD. THE DECIDING OFFICIAL SHOULD NOT DENY THE LICENSE OR EMPLOYMENT BASED ON THE INFORMATION IN THE RECORD UNTIL THE APPLICANT HAS BEEN AFFORDED A REASONABLE TIME TO CORRECT OR COMPLETE THE INFORMATION, OR HAS DECLINED TO DO SO. AN INDIVIDUAL SHOULD BE PRESUMED NOT GUILTY OF ANY CHARGE/ARREST FOR WHICH THERE IS NO FINAL DISPOSITION STATED ON THE RECORD OR OTHERWISE DETERMINED. IF THE APPLICANT WISHED TO CORRECT THE RECORD AS IT APPEARS IN THE FBI'S CJIS DIVISION RECORDS SYSTEM, THE APPLICANT SHOULD BE ADVISED THAT THE PROCEDURES TO CHANGE, CORRECT OR UPDATE THE RECORD ARE SET FORTH IN TITLE 28, CFR, SECTION 16.34.

FBI IDENTIFICATION RECORD -

WHEN EXPLANATION OF A CHARGE OR DISPOSITION IS NEEDED, COMMUNICATE DIRECTLY WITH THE AGENCY THAT FURNISHED THE DATA TO THE FBI.

(10) \*\*\*\*\*NOTICE\*\*\*\*\*  
SUBJECT OF RECORD IS WANTED  
SEE END OF RECORD FOR MORE INFORMATION

END OF PART 1 - PART 2 TO FOLLOW

UNITED STATES DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION  
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION  
CLARKSBURG, WV 26306

USNIGC007Z  
PART 2

NCNE20160000000000000000

FBI IDENTIFICATION RECORD - FBI UCN-000000000

NAME FBI UCN DATE REQUESTED  
SMITH, BRAD 00000000 2016/11/18

SEX RACE BIRTH DATE HEIGHT WEIGHT EYES HAIR  
M W 1954/01/11 603 235 BROBLK

BIRTH PLACE  
TEXAS

PATTERN CLASS CITIZENSHIP  
UNITED STATES  
AU WU RS WU WU AU LS LS WU  
LS RS  
RS

(11)

-----  
\* WANTED \*  
\* \*  
\* CONFIRM THAT WARRANT IS STILL OUTSTANDING \*  
\* \*  
\* AGENCY-SHERIFF'S OFFICE CROWN POINT (IN0450000)  
\*  
\* WANTED-NCIC#W000000000 \*  
\* DAVIS, BRAD \*  
\* FAILURE TO APPEAR - SEE MIS (IDENTIFY \*  
\* ORIGINAL OFFENSE) \*  
\* CASE #0000000 \*  
\* DATE OF WARRANT 01/07/2014 \*  
\* NOTIFY IN0450000 SHERIFF'S OFFICE CROWN POINT IN \*  
-----

RECORD UPDATED 2016/11/18

OFFENDER NAME	STATE ID	FBI NUMBER	NUMBER
SMITH, BRAD		IN0000000	000000000
SEX RACE BIRTH DATE HGT WGT EYES HAIR PLC OF BIRTH			
M	W	1954/01/11	603 235 BRO BLK TX
FINGERPRINT CLASS			

NCIC:  
HENRY UP:  
HENRY LOW:  
NO ALIAS INFORMATION IS ON FILE FOR THIS SID.  
NO SCARS, MARKS, OR TATTOOS IS ON FILE FOR THIS SID.  
SOCIAL SECURITY

000000000

ARREST -01 20130101  
(12) AGENCY: HOBART POLICE DEPT (IN0450900)  
AGENCY CASE: 000000

(13) ARREST CHARGES:  
CHARGE 01:001 OF DWS - PRIOR 1 COUNTS  
CHARGE 02:001 OF FAILURE TO APPEAR 1 COUNTS  
CHARGE 03:001 OF HOLD FOR MERRILLVILLE1 COUNTS

(14) NO DISPOSITION INFORMATION IS ON FILE FOR THIS ARREST  
NO CUSTODY INFORMATION IS ON FILE FOR THIS SID  
THE DATA LISTED ON THE TRANSCRIPT MAY NOT BE AN EXACT REPLICATION  
OF THE DATA SUPPLIED BY THE ARRESTING AGENCY. TO RECEIVE THE EXACT  
CHARGE INFORMATION, A CERTIFIED TRANSCRIPT MUST BE REQUESTED.  
END OF KNOWN RECORD  
END OF RECORD  
\*\*\*END OF RECORD\*\*\*

=====

2.2008:SMITH, BRAD  
2.2031:11

UNITED STATES DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION  
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION  
CLARKSBURG, WV 26306

USNIGC007Z  
PART 2

- FBI IDENTIFICATION RECORD - FBI NO. 123456AZ7

- (15) 1 - ARRESTED OR RECEIVED 1989/07/11  
AGENCY-SHERIFF'S OFFICE RIVERSIDE (CA0330000)  
AGENCY CASE-20987  
CHARGE 1-POSS NARC C/S
- (16) COURT-COUNTY COURT RIVERSIDE  
CHARGE-11350 HS-POSSESS NARCOTIC CONTROL SUBSTANCE  
SENTENCE-  
DIVERSION DISMISSED
- (17) 2 - ARRESTED OR RECEIVED 1995/02/13  
AGENCY-POLICE DEPARTMENT FRESNO (CA0100500)  
AGENCY CASE-8502137001  
CHARGE 1-DRIVING WITH LICENSE INVALID
- 3 - ARRESTED OR RECEIVED 2005/05/26  
AGENCY-POLICE DEPARTMENT CEDAR PARK (TX2460900)  
AGENCY CASE-56302  
CHARGE-AGG ASSAULT SBI
- COURT-26TH DISTRICT COURT GEORGETOWN (TX246015J)  
CHARGE-AGG ASSAULT CAUSES SERIOUS BODILY INJURY  
SENTENCE-  
2006-04-23 DEFERRED PRB-5Y0MOD FNE-2500
- 4 - ARRESTED OR RECEIVED 2011/09/03  
AGENCY-SHERIFF'S OFFICE GEORGETOWN (TX2460000)  
AGENCY CASE-11586  
CHARGE-THEFT>\$20<\$500 BY CHECK
- COURT-COUNTY COURT GEORGETOWN (TX246013J)  
CHARGE-THEFT CLASS C MISDEMEANOR  
SENTENCE-  
2011-12-01 CONVICTED LESSER CHARGE FNE-0200

ALL ARREST ENTRIES CONTAINED IN THIS FBI RECORD ARE BASED ON  
FINGERPRINT COMPARISONS AND PERTAIN TO THE SAME INDIVIDUAL

THE USE OF THIS RECORD IS REGULATED BY LAW. IT IS PROVIDED FOR OFFICIAL  
USE ONLY AND MAY BE USED ONLY FOR THE PURPOSE REQUESTED.

(18)

```
*****CRIMINAL HISTORY*****
===== CYCLE 1 =====
Tracking Number      1463714637
Earliest Event Date  1997-03-01
-----
Arrest Date          1997-03-01
Arresting Agency     CO0340100 DURANGO POLICE DEPARTMENT
Subject's Name
Comment(s)           MNU#: OA-970000
Charge               1
Charge Literal       ASSAULT
Statute              ASSAULT 3RD DEG (1399)
Counts               1
Severity              MISDEMEANOR
```

(19)

```
*****CRIMINAL HISTORY*****
===== CYCLE 001 =====
TRACKING NUMBER      00066384102
EARLIEST EVENT DATE  2001-03-21INCIDENT DATE      2001-03-21
-----
```

(20)

```
ARREST CASE NUMBER   10301 6E
ARRESTING AGENCY     GA0460100 VIENNA POLICE DEPARTMENT
SUBJECT'S NAME
ARREST TYPE          ADULT
CHARGE               1
CHARGE NUMBER        00066384102001
CHARGE TRACKING NUMBER 0066384102
CHARGE LITERAL       DISORDERLY CONDUCT
STATUTE              DISORDERLY CONDUCT {16-11-39; GA)
STATE OFFENSE CODE   5311
SEVERITY              MISDEMEANOR
-----
```

```
COURT DISPOSITION    {CYCLE 001)
COURT AGENCY          GA046031J VIENNA RECORDERS COURT
SUBJECT'S NAME
CHARGE               1
CHARGE NUMBER        00066384102001
CHARGE TRACKING NUMBER 00066384102
CHARGE LITERAL       DISORDERLY CONDUCT
STATUTE              DISORDERLY CONDUCT {16-11-39; GA)
STATE OFFENSE CODE   5311
SEVERITY              MISDEMEANOR
DISPOSITION          {CONVICTED 2001-04-18; BOND FORFEITURE)
```

<CRIMINAL HISTORY INFORMATION>

```
LAST ARRESTED:      01/19/1997
ARREST AGENCY:      HONOLULU PD
TOTAL ARRESTS:      2
TOTAL CHARGES:      2
ARREST: 1 OF 2
ARREST DATE/AGENCY: 01/19/1997      HONOLULU PD
OBTS TRACKING NUMBER: 30261H4
CRIME TYPE:
CHARGE: 1 OF 1
CHARGE              STATUTE              SV              FC
ARREST/FILING:     ASSAULT 2              707-0711        SV              FC
FINAL/LAST:         ASSAULT 2              707-0711        SV              FC
ARREST REPORT:     97-025036
(SV = SEVERITY FC=FELONY CLASS C)
FINAL/LAST: AGENCY: HONOLULU FAM CT
CASE NO: FC97-0001
DISP/DATE: GUILTY              05/06/1997
DAGRETURN:
SENTENCE:           ON 05/06/1997, SUBJECT WAS SENTENCED TO 50 HOUR(S)
COMMUNITY SERVICE, 5 YEAR(S) PROBATION, AND $372
RESTITUTION.
```

\*\*\*\*\* CRIMINAL HISTORY \*\*\*\*\*

===== CYCLE 001 =====

Tracking Number 00000000100  
Earliest Event Date 2004-12-03 Incident Date 2005-01-11

Arrest Date 2005-01-11  
Arresting Agency KS0260000 ELLIS COUNTY SHERIFF'S OFFICE HAYS

Subject's Name  
Arrest Type Adult  
Comments Fingerprinted on 2005-01-11.

Charge 1  
Charge Literal Worthless check; Unknown value  
Charge Description Non-Person Offense  
Statute Giving a worthless check; Unknown value  
(21-3707 KS)  
Counts 1  
Severity Unknown  
Disposition Other(Referred to prosecutor.)

Booking Case Number 05-025

Prosecutor Disposition (Cycle 001)  
Prosecutor Case Number 04CR000  
Prosecution Date 2004-12-03  
Prosecutor Agency KS026013A ELLIS COUNTY ATTORNEY'S OFFICE HAYS  
Subject's Name

Charge 1  
Charge Literal Worthless check; Misd  
Charge Description Non-Person Offense  
Statute giving worthless check; Misdemeanor (21-3707 KS)  
Counts 1  
Severity Misdemeanor Class A

Disposition Diversion(Diversion completed)  
Prosecution Comment Diversion initiated on 2005-01-11. Diversion  
Period 6 months. Diversion completed on  
2005-07-11.  
Prosecution Comment Dismissed with prejudice 07/11/05

\*\*\*\*\*CRIMINAL HISTORY\*\*\*\*\*

===== CYCLE 001 =====

Tracking Number 001  
Earliest Event Date 2002-12-15

Arrest Date 2002-12-15  
Arrest Case Number 2702027020

Arresting Agency FL0069000  
FLORIDA HIGHWAY PATROL - FT.

LAUDERDALE  
Arrest Type ADULT  
Charge 001  
Charge Number 2702027020  
Charge Tracking Number 060701060701  
Charge Literal DUI-UNLAW BLD ALCH-  
Agency FL0069000  
FLORIDA HIGHWAY PATROL - FT.

LAUDERDALE  
Charge Description DUI ALCOHOL OR DRUGS 1ST OFFENSE  
Statute DUI ALCOHOL OR DRUGS (FL316.193(2A);FL

(21)

)

NCIC Offense Code 5407  
Counts 001  
Severity MISDEMEANOR  
Enhancing Factor 2ND DEGREE

-----  
Prosecutor Disposition (Cycle 001)  
Prosecution Date 2002-12-15  
Prosecutor Agency FL006023J BROWARD COUNTY COURT  
Charge 001  
Charge Number 001  
Charge Tracking Number 060701060701  
Charge Literal DUI-UNLAW BLD ALCH-  
Charge Description Suppl Arr Degree:1ST  
Charge Description Suppl Arr Level:MISDEMEANOR  
Charge Description DRIVING UNDER THE INFLUENCE  
Charge Description COUNSEL TYPE:OTHER  
Statute DUI ALCOHOL OR DRUGS (FL316.193(1);)  
NCIC Offense Code 5407  
Counts 001  
Severity MISDEMEANOR  
Enhancing Factor 1ST DEGREE  
Disposition (Other 2003-01-15; FILED  
)

-----  
Court Disposition (Cycle 001)  
Court Disposition Date 2003-01-21  
Court Case Number 0000000000001MI  
Court Agency FL006023J  
BROWARD COUNTY COURT  
Charge 001  
Charge Number 001  
Charge Tracking Number 060701060701  
Charge Literal DUI-UNLAW BLD ALCH-  
Charge Description DRIVING UNDER THE INFLUENCE  
Charge Description COUNSEL TYPE:OTHER  
Charge Description TRIAL TYPE:NONE  
Charge Description PLEA TYPE:NOLO CONTENDRE  
Statute DUI ALCOHOL OR DRUGS (  
FL316.193(1)  
;)

NCIC Offense Code 5407  
Counts 001  
Severity MISDEMEANOR  
Enhancing Factor 1 ST DEGREE  
Disposition (Convicted 2003-01-21; GUILTY/CONVICTED  
)

-----  
Sentencing (Cycle 001)  
Sentence Date 2003-01-21  
Sentencing Agency FL006023J BROWARD COUNTY COURT  
Court Case Number 0000000000001MI  
Charge 001  
Charge Number 001  
Charge Literal DUI-UNLAW BLD ALCH-  
Sentence  
PROBATION-06M  
Sentence  
FINE- \$263.00  
Sentence  
COURT COST- \$26.00  
Sentence  
COURT PROVISION - COMMUNITY SERVICE  
Sentence

COURT PROVISION - ATTEND DWI SCHOOL

Sentence

COURT PROVISION - ABIDE BY COURT RESTRICTIONS

===== CYCLE 002 =====

Tracking Number                    002

Earliest Event Date                2012-08-29 Incident Date    2012-08-29

-----

Arrest Date                         2012-08-29

## Section 3 - Basic Privacy & Security Guidelines

Access, use, handling, dissemination, and destruction of criminal justice information (CJI) and criminal history record information (CHRI) is governed by federal and state laws, rules, regulations and policies. The receiving organization is responsible for maintaining the confidentiality and control of any CJI/CHRI it obtains.

CJI/CHRI may only be used for the specific purpose for which it was requested (employment, licensing, volunteers, etc.). For more information regarding the FBI CJIS Security Policy please visit <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center>. The policy is updated periodically so the Tribe must check the website often to ensure the correct FBI CJIS Security Policy is being used. Sample policies for Proper CHRI Access, Use, Handling and Dissemination can be found in Appendix F.

### 3.1 Policies and Procedures

The Tribe must establish policies/procedures in the following CJI/CHRI privacy and security areas, and ensure all organization personnel are aware of them.

- Access:
  - Defining who is authorized to access CJI/CHRI (Authorized Personnel)
  - Restricting access to only those who are authorized
- Use:
  - Defining the authority, purpose and use of the CJI/CHRI. In the case of CJI/CHRI obtained through NIGC via IGRA, the purpose and use is for licensing and/or employment of key employees and primary management officials of tribal gaming enterprises, as defined by NIGC regulations.
  - Restricting use to the specific purpose for which the CJI/CHRI was requested
- Handling:
  - Proper security of CJI/CHRI from receipt through destruction
  - Retention/destruction rules and processes
- Prevention of unauthorized disclosure of CJI/CHRI:
  - Access-limited storage
  - Not leaving CJI/CHRI unattended when it is not physically secured
  - Revocation of access privileges for terminated employees or those removed from the Authorized Personnel List
  - Processes for ensuring proper training and refresher training of Authorized Personnel
- Communication:
  - Communication among Authorized Personnel
  - Communication with the applicant concerning CJI/CHRI, including the provision of the FBI Privacy Act Statement (dated 2013 or later) and *Noncriminal Justice Applicant's Privacy Rights* notice as well as written notification of the procedures for obtaining a change, correction, or update to their criminal history record as set forth in 28 C.F.R. § 16.34 and the provision of a reasonable amount of time to do so.
- Secondary dissemination procedures (if permitted by law):
  - Tribes may provide an applicant or the applicant's attorney a copy of their criminal history record if the tribe has established a written policy to do so
  - Otherwise, generally, secondary dissemination – or reuse – of CJI/CHRI obtained through the NIGC is not permitted.
  - Logging/tracking procedures
  - Procedures for authenticating recipients of the disseminated information
- Formal disciplinary procedure:
  - Steps to be taken by the organization in the event of misuse of CJI/CHRI
  - Specify applicable misconduct policies

- Digital security (if CJI/CHRI scanned or stored electronically):
  - Technical safeguards to protect the access and integrity of confidential information
  - Monitoring and restricting access to databases containing CJI/CHRI, including employing required identification and authentication measures
  - Reporting, response, and handling capability for information security incidents
  - Employing a formal sanctions process for personnel that fail to comply with information security policies and procedures, including those mandated by the CJIS Security policy
  - Ensuring all Authorized Personnel have taken the requisite security awareness training in accordance with the CJIS Security policy
  - Undertaking information technology security audits in accordance with the CJIS Security policy

Additionally, Agencies must have established processes for fingerprint submissions which include:

- Quality assurance measures for applicant identity verification. (See Section 2.2)
- Quality assurance measures for protecting the integrity of the fingerprint card. (See Section 2.12)
- Processes to ensure compliance with federal laws for FBI fingerprint checks (if applicable). (See Section 2.3)

The Tribe must consider the following basic guidelines when formulating policies, procedures, and training.

### **3.2 Applicant Process**

It is the policy of the NIGC to allow the tribe to discuss and provide the criminal record contents with the applicant within the confines of the purpose for which it was provided (i.e. licensing and/or employment of key employees and primary management officials of tribal gaming enterprises):

- The tribe may tell the applicant that there is a factor in the criminal history check that may be disqualifying and discuss that factor with the applicant in order to ascertain if the circumstances of the issue warrant denial.
- To facilitate the challenge/correction process, NIGC permits tribe to supply the applicant or the applicant's attorney 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. (See Section 3.3)

### **3.3 Applicant Review and Challenge of Criminal History**

It is the tribe's responsibility to notify applicants in writing of the opportunity and ability to review and challenge their criminal history record. If an applicant believes that their criminal history record is inaccurate or incomplete, refer the person to one of the options below to begin the review and challenge process.

- For a copy of an FBI criminal history record directly from the tribe:
  - The tribe must have adopted written policies and procedures that allow the subject of an FBI record to request a copy of their own record. The policy must include how the request is made; the amount of time to provide the report; how the report will be provided and, if provided by the tribe, how it will be marked to distinguish it as a copy; verification of the applicant's identity; and when the report was provided. Additionally, the Tribe must provide a reasonable amount of time for the applicant to complete or correct the report before the final licensing or employment determination is made. Ensure the applicant is aware that the CHRI provided to the applicant MAY NOT be reused for employment or licensing purposes by any other entity or agency.
- For a copy of an FBI criminal history record directly from the FBI:

- Federal law and U.S. Department of Justice regulations allow the subject of an FBI record to request a copy of their own record. The individual may submit fingerprints, an Applicant Information Form, and payment directly to the FBI according to the procedures in Title 28 C.F.R. §16.30 - 16.34.
- FBI contact phone for information about record review and challenge: (304) 625-5590.
- Submittal forms, checklists, and more information on how to review and challenge an FBI criminal history record can be found at **www.fbi.gov** under *Criminal Justice Information Services - Identity History Summary Checks*.

If the Tribe received their CHRI from a State, rather than NIGC, and that State specifically prohibits release of CHRI, the applicant **must be referred** to that State for a copy of the State CHRI and to FBI for a copy of the FBI CHRI. Note: Arizona prohibits release of CHRI obtained through their services to applicants.

### 3.4 Communication/Dissemination

Verbal or written communications regarding CJI/CHRI may only occur between Authorized Personnel and only to carry out the specific purpose for which the information was requested. In the case of CJI/CHRI obtained through the NIGC that purpose is licensing and/or employment of key employees and primary management officials of gaming enterprises, as such are defined in NIGC regulations.

#### 3.4.1 Communication Cautions

Tribal personnel must be aware of the following restrictions and cautions concerning CJI/CHRI:

- CJI/CHRI received from the fingerprint criminal history check process is not public record and may not be released to the public. The tribe may neither confirm nor deny the existence or nonexistence of an individual's criminal history record to the public or to any unauthorized individual or tribe.
- Care must be taken to prevent overhearing, eavesdropping, or interception of communication. Consider using private rooms, closed offices, etc., when discussing CJI/CHRI with other authorized personnel or with applicants.
- Viewing and/or disseminating CJI/CHRI for curiosity reasons is not allowed.
- CJI/CHRI cannot be:
  - Emailed (unless encrypted to CJIS Security Policy standards)
  - Sent electronically via cell phone or other handheld device (including texts or pictures of the hardcopy or computer screen)
  - See FBI CJIS Security Policy at <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center> for Bring Your Own Device (BYOD) requirements
- CJI/CHRI may be faxed only if:
  - The recipient point is within the tribe or secondary dissemination is authorized. As noted above, secondary dissemination is generally not authorized. (See Section 3.1 & 3.4.2).
  - The recipient has been confirmed by the sender as Authorized Personnel or as an otherwise authorized recipient.
  - The receiving fax is in a secure location controlled by the authorized recipient and the arriving CJI/CHRI is not accessible to unauthorized personnel. The tribe is responsible for the security of all copies of CJI/CHRI.
  - See FBI CJIS Security Policy at <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center> for encryption requirements
- Personnel must be cautioned regarding common causes of casual unauthorized release of

information: e.g., social networks, discussions with friends/family members, conversations in public places.

- Personnel must be made aware of the threat of social engineering. Social engineering is deliberate manipulation or deception designed to elicit the release of confidential information to unauthorized individuals. If secondary dissemination is permitted, the tribe must develop a method which allows personnel to verify the identity and authorized status of an individual requesting information both inside and outside the tribe.

### 3.4.2 Secondary Dissemination

The receiving tribe may not provide CJI/CHRI to any other tribe, state, agency or individual unless specifically authorized by law. This is called “secondary dissemination” or “reuse”. To be clear, IGRA does not provide for such secondary dissemination or reuse. And CJI/ CHRI obtained through the NIGC cannot be improperly disseminated beyond tribal personnel directly involved in the key employee and primary management official licensing or employment deliberations.

If permitted by other federal or state law, secondary dissemination can only occur with an authorized recipient. All secondary dissemination must be logged, and the log shall be retained for three years. The log must clearly identify the following:

- a) Date of dissemination
- b) Name of requestor
- c) Name and contact information of requestor’s tribe
- d) Purpose for which information is requested
- e) Specific information being released (i.e., criminal history of name of subject)
- f) The name/identification of the person releasing the information

**Do not assume you can disseminate the CHRI, please verify your authorization. There are civil and criminal penalties for unlawful dissemination.**

## 3.5 Physical Security

The Tribe is responsible for the security of the CJI/CHRI from its arrival at the tribe through the point of its complete destruction.

### 3.5.1 Storage

The results of the FBI record search must be stored in such a manner that only authorized personnel have access and must not be retained longer than needed to fulfill its purpose and satisfy the tribe's regulatory guidelines.

- CJI/CHRI must be maintained at all times in a secure location to prevent access/viewing by unauthorized personnel (i.e., locked file cabinet, locked room, secure perimeter, etc.).
- All visitors (including contractors, maintenance, and outside personnel) to areas where CJI/CHRI is kept must be accompanied by Authorized Personnel at all times. Areas must be locked when unattended. Additionally, check the identification of all visitors, contractors and anyone not on the authorized personnel list who may be entering the restricted, controlled area where CHRI is stored or used.
- Authorized Personnel who are granted access to CJI/CHRI must be aware of their responsibility to protect the confidentiality of the information and take steps accordingly. Examples of this are: turning pages with CJI/CHRI face down on a desk; not leaving information exposed or unattended; turning or covering computer screens to inhibit casual viewing; being aware of

unauthorized individuals who may be “shoulder surfing” or walking by when information is being viewed.

### **3.5.2 Destruction**

When no longer needed for its purpose, CJI/CHRI must be completely destroyed to minimize the risk of unauthorized access and dissemination. Please review NIGC regulations at 25 C.F.R. §556.6(a) and 25 CFR §558.3(e) and the approved tribal gaming ordinance for retention time requirements.

- CJI/CHRI cannot simply be thrown away. The acceptable methods of destruction are shredding or incineration.
- Electronic media holding CJI/CHRI must first be sanitized (overwritten at least three times, degaussed) prior to complete destruction.
- Destruction must be performed or observed by Authorized Personnel who are authorized to access/handle CJI/CHRI or approved outsourced contractors (See Section 1.4).

### **3.6 Technical/Digital Security**

If the CJI/CHRI sheets are stored electronically, or CJI/CHRI derived from the sheets is stored electronically, then the Tribe becomes subject to technical information security requirements.

The requirements for electronic storage and access of CJI/CHRI are contained in the FBI CJIS Security Policy and are in the online FBI CJIS Security Policy Resource Center on the FBI website at <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center>. Electronic security, encryption, and storage protection requirements in the policy apply to TGRAs converting hardcopy CJI/CHRI into electronic format after receipt; the parts governing direct connect/interface with the state/national electronic criminal justice databases do not apply unless the TGRA has an additional function with direct connect/interface access. TGRAs must have knowledgeable information technology (IT) personnel review the requirements in the Security Policy and ensure that TGRA's system is in compliance.

The following general guidelines also apply to electronic/digital security of CJI/CHRI:

- 1) Criminal Justice Information (CJI/CHRI) must be encrypted:
  - When stored (at rest) outside the boundary of a physically secure location
    - When encryption is used for CJI/CHRI 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 in the FBI CJIS Security Policy)
    - When encryption is used for CJI/CHRI in transit, it must be FIPS 140-2 certified and use a symmetric cipher of at least 128 bit.
- 2) The server must be secure and located on-site either with that Tribe or on a site controlled by the Tribe.
  - The actual location of the computers and servers must have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment or to any of the stored data.
  - Only Authorized Personnel of the TGRA may have access to the server. IT Personnel who are not Authorized Personnel and have unescorted access to unencrypted CJI/CHRI need FBI Compact Officer approved Outsourcing Agreements. (See Section 1.4)

- See FBI CJIS Security Policy for Cloud storage requirements.
- 3) Authorized Personnel who access CJI/CHRI electronically must complete Level Three of the CJIS Security Awareness Training that pertains to electronic access. Authorized Personnel who maintain electronic CJI/CHRI systems must complete Level Four CJIS Security Awareness Training.
  - 4) The Tribe must manage information system accounts. Requirements include:
    - Processes for activating, reviewing, and disabling accounts.
      - The files where CJI/CHRI is stored must be password-protected.
      - Each individual accessing the CJI/CHRI files must be uniquely identified and have a unique password.
      - Password rules are detailed in the FBI CJIS Security Policy.
    - Processes for authorizing and monitoring remote access (if applicable).
    - Restrictions regarding the use of personally owned electronic devices to access, handle, or store CJI/CHRI.
    - Electronic media protection rules, to include provisions for destruction, which include degaussing, overwriting, or physical destruction of media. (See Section 3.5.2)
  - 5) The computer system must include protective features detailed in the CJIS Security Policy. These include but are not limited to:
    - Partitioning which physically or logically separates user interface services from information storage databases
    - Intrusion detection/malicious code protection
    - Spam and spyware detection/protection
  - 6) A security incident handling policy must be in place that allows users to alert technical personnel to an information security incident such as an unauthorized system intrusion. The incident handling response must include preparation, detection, analysis, containment, eradication, and recovery. Each incident must be tracked and documented, including user response activities.
  - 7) When an incident occurs, a Security Incident Report form must be completed and submitted to the NIGC ISO **within 24 hours** of discovery of the incident. The submitted report must contain a detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident. The NIGC uses the CJIS Security Appendix F.1 form to report these incidents. A copy of the form can be found in Appendix F.

### **3.7 Consequences for Misuse**

The receiving tribe/TGRA has the responsibility to ensure that all personnel are aware of the consequences that may result from unauthorized use of CJI/CHRI.

Federal statutes state that access to CJI/CHRI is subject to cancellation for dissemination outside the authorized recipient(s) (Title 28 U.S.C. §534 and Title 28 C.F.R. §20.33). A Tribe's access to CJI/CHRI via submitted fingerprints may also be suspended or cancelled according to the terms and conditions in the MOU.

Other federal and/or state penalties may apply depending on the circumstances of the release and the specific statute violated. Two examples of United States Code violations are Title 18 U.S.C §641 which deals with theft of public records for personal gain and Title 18 U.S.C §1030 which discusses unauthorized access to protected information via computer.

Unauthorized release could potentially expose the organization and/or individual to civil liability. In addition, an individual may be subject to disciplinary action under his/her employer's misconduct policies.

## Section 4 - LASO Responsibilities

As mentioned in Section 1 of this guide, the new Memorandum of Understanding (MOU) will require each tribe to designate a Local Agency Security Officer (LASO). The LASO is the primary liaison between the tribe and the NIGC and is responsible for coordinating tribal compliance with all federal and state laws and regulations pertaining to the access, use, handling, dissemination, and destruction of CJI and CHRI. This section summarizes the primary duties and responsibilities of the LASO. A LASO responsibilities handout can be found in Appendix G.

### 4.1 Primary Liaison

The LASO functions as the primary liaison with the NIGC for all communication regarding audits, training, and security. The LASO is also the first point of contact for the NIGC in the event of an allegation of criminal history misuse or a security issue involving the criminal history check process. It is important that the LASO's contact information stay updated with the NIGC in order to allow for orderly and timely exchange of information.

The LASO is also expected to serve as the information resource for his/her TGRA. The NIGC will send periodic emails to the LASO to keep agencies updated on changes and events relevant to the noncriminal justice process. The LASO is expected to share this information with the personnel at the TGRA as needed.

The NIGC also maintains a contact person at each TGRA in case of a processing problem. TGRAs may choose to have the LASO serve in both capacities or may choose to have a different person for each, based on the Tribe's organizational structure and need. Both contacts must be kept updated.

#### 4.1.1 Information Changes

In addition to keeping the LASO's contact information updated, the LASO is responsible for keeping the tribe and TGRA's information updated. The LASO must inform the NIGC of changes in the authorized Tribal signatory on the MOU, the LASO, or any relevant business information (Tribe name changes, mailing/physical address changes, etc.). The forms mentioned in this section are in the appendices of this guide and are also available from the NIGC website at <https://www.nigc.gov/compliance/CJIS-Training-Materials>. Forms may be emailed, faxed, or mailed to the NIGC ISO. (See the Contact List on page 5).

If the signatory to the MOU changes:

- The tribe must sign a new MOU within 6 months or access will be suspended.

If the LASO changes:

- The tribe must appoint a new LASO and submit the *Noncriminal Justice Agency Information Change Form* to the NIGC within 30 days of the change. (See Appendix H for a copy of this form or the NIGC website at <https://www.nigc.gov/compliance/CJIS-Training-Materials>.)
- The tribe can also designate a secondary (backup) LASO on this form.
- The NIGC will send an email acknowledgment upon receipt of the notification.

If the authorized Tribal signatory changes:

- Submit the *Noncriminal Justice Agency Information Change Form* to the NIGC. (See Appendix H or the NIGC website at <https://www.nigc.gov/compliance/CJIS-Training-Materials>.) If a new authorized tribal signatory has not been selected, submit the information of the interim/acting authorized signatory and note the anticipated time before permanent replacement in the form's Comments field.

- The NIGC will provide a MOU with instructions for its completion if needed.

If the name, mailing address, physical address, and/or main phone number of the tribe changes:

- Fill out the information you want to change on the *Noncriminal Justice Agency Information Change Form*. (See Appendix H or the NIGC website.)
- The NIGC will acknowledge receipt of the form and update the information. If further information is required, the NIGC will contact the LASO with any questions.

#### **4.1.2 Authorized Personnel List**

The LASO must submit an Authorized Personnel List to the NIGC. The Authorized Personnel List contains all TGRA and tribal personnel who are authorized to receive, view, handle, disseminate, store, retrieve, or dispose of CJI/CHRI. The Authorized Personnel List must be submitted by the tribe and must contain the names and titles of the authorized individuals.

Examples of types of personnel a tribe and TGRA may want to authorize:

- Administrative personnel who open the tribe's mail, have filing duties, or perform functions which grant them trusted access to locked/secured areas or access to unsealed CJI/CHRI.
- Personnel involved in licensing eligibility determinations: Gaming Commissioners, Executive Directors, Licensing agents, etc.
- TGRA Information technology personnel (if CJI/CHRI is stored electronically). Please note, IT Personnel who are not Authorized Personnel and have unescorted access to unencrypted CJI/CHRI need FBI Compact Officer approved Outsourcing Agreements. (See Section 1.4)

An example Authorized Personnel List can be found in Appendix I of this guide and also online on the NIGC website at <https://www.nigc.gov/compliance/CJIS-Training-Materials>. The entire Authorized Personnel List must be updated and resubmitted when changes occur (e.g., an individual is no longer authorized to view/handle CJI/CHRI, an authorized individual is no longer employed by the tribe or TGRA, an authorized individual has a name change, personnel turnover, and name/contact information changes). Ensure the LASO is on the Authorized Personnel List. The tribe must retain one copy of the Authorized Personnel List for its records and forward a copy to the NIGC.

## **4.2 Privacy and Security Coordinator**

The LASO is the person primarily responsible for maintaining Tribe compliance with federal and state law and regulations for privacy and security requirements. Compliance duties include:

- Ensuring Authorized Personnel receive required training.
- Updating/maintaining training documentation.
- Updating and submitting Authorized Personnel List to NIGC.
- Ensuring Authorized Personnel have signed the Tribe's Acknowledgement Statement.
- Ensuring the Tribe has adequate policies/procedures related to access, use, handling, dissemination, and destruction of CJI/CHRI.

### **4.2.1 Required Training for Authorized Personnel**

Authorized Personnel must complete two sets of training:

#### 1) CJIS Training:

CJIS Security Awareness Training (SAT) required for all individuals (criminal justice and noncriminal justice) who view or handle CJI and CHRI. All Authorized Personnel must receive CJIS SAT within six months of hire or being placed on the Authorized Personnel List and then every two years thereafter. SAT is designed to explain and clarify points for those individuals who have no background in the criminal justice field. There are four levels of CJIS security awareness training required for each person's access and duties. Level One is for persons with unescorted access to a physically secure location; Level Two is for all authorized personnel with access to CJI; Level Three is for all authorized personnel with both physical and logical access to CJI; and Level Four is for all

Information Technology personnel.

A copy of the FBI CJIS SAT PowerPoint Presentation and a 30 minute NIGC Licensing Update video can be found at the NIGC website at <https://www.nigc.gov/compliance/CJIS-Training-Materials>.

2) Tribe's policies/procedures training:

Each tribe must train Authorized Personnel on the Tribe's internal policies/procedures for the proper access, use, handling, dissemination, and destruction of CJI/CHRI and on the consequences of misuse of CJI/CHRI. This training must be conducted within six months of hire or being placed on the Authorized Personnel List and then every two years thereafter. The Tribe will be required under the new MOU to have the internal security incident handling procedures; more information on the required policies/procedures is available in Section 3.1 and Section 5.2. The LASO must ensure that the training curriculum is adequate and covers the required topics. Training outlines will be reviewed by the NIGC during audits.

As discussed above, the LASO is responsible for maintaining and updating the Training Documentation Form showing that both CJIS Online and tribal internal privacy and security training have been completed. NIGC's compliance training is designed to help the LASO or other designated tribal/TGRA representative understand the new compliance requirements so that they can implement the rules back at their Tribe and TGRA; NIGC training does not take the place of the tribe's internal training. The Tribe/TGRA must document each instance when its Authorized Personnel receive this training and retain documentation for a minimum of two years. Upon request, it must be forwarded to the NIGC. A blank Training Documentation Form is located in Appendix J of this guide and is also available for download at the NIGC website at <https://www.nigc.gov/compliance/CJIS-Training-Materials>.

#### **4.2.2 Acknowledgement Statements**

All authorized personnel must sign a statement acknowledging notification of the penalties for misuse of the CJI and CHRI. There is no standard format for the Acknowledgement Statement. It must state at a minimum that the undersigned "acknowledges notification for the penalties for misuse of criminal justice and criminal history record information," but ideally it contains a summary of state, federal, and tribal consequences. TGRAs may choose to add a short training outline to the statement so that the employee specifically acknowledges their training as well.

The LASO is responsible for entering the date Acknowledgement Statements were signed on the Training Documentation form. Do not send the acknowledgement statements to the NIGC; keep the forms on file at the TGRA/tribe. NIGC personnel will review these forms during the tribe's audit.

#### **4.3 Audit Responsibilities**

The LASO is the tribe's representative for all audits and cooperates with federal and state officials throughout the audit process. More details on the audit process are contained in Section 5.

The LASO's responsibilities during an audit include:

- Ensuring all the audit instructions are followed and that the audit packet is returned in a timely manner.
- Being present for the audit interview and notifying/gathering any other TGRA/tribal personnel who may be needed to answer the auditor's questions.
- Having all requested documentation available for the audit.
- Serving as the primary coordinator for any corrective actions stemming from the audit findings.

## Section 5 - Audits & Compliance

TGRAs who utilize the NIGC fingerprint submission program are subject to an audit by the NIGC and the FBI to ensure compliance with federal rules regarding fingerprint submissions and CJI/CHRI use. The FBI Audits include the Noncriminal Justice Information Technology Security (NCJITS) Audit and the National Identity Services (NIS) Audit. This section explains the general audit process and discusses the FBI CJIS and NIGC requirements. A Compliance checklist and IT checklist can be found in Appendix K.

### 5.1 Audits

A routine audit cycle has been established for noncriminal justice agencies in order to assess compliance with tribal and federal policies and regulations. For NIGC audits, NIGC personnel will conduct the audits.

#### 5.1.1 Routine Audits

A routine audit is a scheduled review of the Tribe's compliance with the FBI CJIS and NIGC requirements. The NIGC will notify the Tribe approximately 30 days in advance of the planned audit date. The notification will describe the audit process and provide the contact information of the assigned NIGC Compliance Officer. The LASO should contact the NIGC Compliance Officer to acknowledge receipt of the audit notification.

The notification will state whether the Tribe is scheduled for a telephonic or an in-person audit. The LASO must be present for the audit; the Tribe may also have other personnel in attendance if needed or desired. Compliance assessment documents will be sent with the notification; these documents will need to be completed and returned by the date indicated on the accompanying audit timeline.

The NIGC Compliance Officer will conduct a complete file review of the TGRA/tribe prior to the audit interview. All documentation relating to general administration, fingerprint submissions, privacy and security, and training will be reviewed at or before the audit interview. The LASO will be asked to complete an assessment questionnaire and a chart as part of the pre-interview process.

After an audit has been completed, the NIGC Compliance Officer will provide the TGRA/tribe with a written report which will either denote complete compliance or will contain recommendations for corrective actions to bring the TGRA/tribe into compliance. NIGC Compliance Officers are available to discuss specific concerns and to offer training to assist the TGRA/tribe in this process.

#### 5.1.2 Directed Audits

A directed audit is an administrative review prompted as a result of an incident or allegation of possible misuse of CJI/CHRI. Most issues of misuse stem from instances of improper dissemination of criminal history record information to unauthorized individuals or agencies.

The NIGC may conduct a directed audit of a Tribe if the NIGC:

- Receives a complaint from a Tribe or individual alleging misuse of CJI/CHRI.
- Becomes aware of Tribal actions which may constitute a misuse of CJI/CHRI.
- Becomes aware of Tribal actions which may be a violation of the MOU terms.

A NIGC Compliance Officer will contact the tribe's LASO and arrange to conduct a review of the TGRA/tribe's processes and actions which may have resulted in a misuse. If the Compliance Officer cannot reach the LASO within a reasonable period of time, they will contact the LASO's supervisor, authorized tribal official on the MOU, or other administrator.

The review by an NIGC Compliance Officer is designed to detect process issues that may result in noncompliant actions by a TGRA/tribe. Areas audited are the same as those checked during a routine audit, and the review may focus on the policies, procedures, process, and actions most closely related to the allegation. NIGC Compliance Officers will ask questions regarding the circumstances surrounding the allegation to determine if/how the incident occurred and what actions might be required to prevent a repeat of any misuse. The LASO should be present for the audit as well as any other personnel the TGRA/tribe deems necessary. Following the directed audit, the NIGC Compliance Officer will prepare a written report of their findings. If compliance issues are detected, the report will contain recommendations and/or specific requests in order to bring the TGRA/tribe into compliance so that it can continue to utilize the fingerprint criminal history check process through the NIGC. The Tribe will be required to respond in writing regarding its corrective actions in the areas of concern.

A directed audit does not replace a routine audit. If a directed audit finds issues that require correction, a TGRA/tribe may be scheduled for a routine audit after a specified period to reassess its compliance.

## **5.2 Compliance Review**

This subsection discusses the general compliance requirements for each of the areas reviewed by NIGC Compliance Officers: general administration, fingerprint submissions, privacy and security, and training. Each part contains a short explanation of the requirements and may reference different resources or areas of the guide which a TGRA/tribe may refer to for more information.

### **5.2.1 General Administration**

The general administration section of an audit reviews the basic information on file for the TGRA/tribe for completeness, accuracy, and compliance with current regulations.

- 1) Memorandum of Understanding (Section 1.2)  
The MOU is the contractual agreement between the tribe and the NIGC that allows the NIGC to provide CJI/CHRI upon submission of fingerprints. Changes to the signatory to the MOU may be a reason that the MOU needs to be updated. The LASO's duties regarding information changes are detailed in Section 4.1.1.
- 2) Authorized Personnel List (Section 4.1.2)  
The LASO is responsible for maintaining an updated Authorized Personnel List on file with the NIGC. The Authorized Personnel List contains those individuals whom the TGRA/tribe has identified as authorized to access, handle, and/or destroy CJI/CHRI. The authorizations are based solely on the TGRA/tribe's determination, but must be limited to the minimum number of personnel necessary. **ALL** personnel who view, handle, use, disseminate, or dispose of CJI/CHRI **MUST** appear on the list; the list will be checked at every audit.
- 3) Tribe File Information (Section 4.1.1)  
The LASO must inform the NIGC in writing of changes in the authorized tribal signatory on the MOU, the LASO designation, or any relevant business information (tribe name changes, mailing/physical address changes, etc.). The NIGC Compliance Officer will check that all the information on file at the NIGC is current. Make changes as they occur – do not wait for an audit!
- 4) Authorization and Purpose (Section 1.2, Section 1.3, Section 2.13.1 #17)  
Each fingerprint submission access is for a specific purpose and is pursuant to a specific authorization. Fingerprints cannot be submitted for any purpose other than that which is named in the tribe's authorization. The NIGC Compliance Officer will check the tribe's authorization

and verify each purpose.

### 5.2.2 Fingerprint Submissions

The NIGC Compliance Officer will review the tribe's entire fingerprint submission process covering properly filling out the cards, applicant identification, processes to protect the fingerprint card from tampering, and notifications and disclosures to the applicant.

- 1) Proper Citing of the “Reason Fingerprinted” (Section 2.13.1 #17)  
Fingerprint cards may only be submitted for specific purposes under approved authorizations. In the “Reason Fingerprinted” box on the card, TGRAs are required to specify the particular purpose for the submission – “Indian Gaming License or Employment of a Key Employee or Primary Management Official”
- 2) Applicant Identification (Section 2.2)  
TGRAs must have processes for verifying the identity of the applicant at the time of fingerprinting. The NIGC Compliance Officer will check for procedures, which include:
  - Informing fingerprinting personnel of the identification requirement.
  - Requiring proper identification at the time of fingerprinting.
- 3) Protection of the Fingerprint Card Prior to Submission (Section 2.12)  
Agencies must have processes for protecting the integrity of the fingerprint card and preventing tampering with the card from the time the prints are taken through the submission to the NIGC. The NIGC Compliance Officer will look for procedures which establish either a process that prevents the applicant from possessing a completed fingerprint card or prevents direct access to the card (such as a sealed envelope system). The processes must also include instructions to fingerprinting personnel as necessary.
- 4) Review and Challenge Notification (Section 3.3)  
It is the TGRA/tribe’s responsibility to notify applicants in writing of the opportunity and ability to review, correct, update, and/or challenge a criminal history record. Also applicants must be provided a reasonable amount of time to do so before a final licensing and/or employment decision is made. Review and challenge contact information is in Section 3.3 of this guide.
- 5) FBI Applicant Privacy Rights Notifications and FBI Privacy Act Statement (Section 2.3)  
Any tribe which submits fingerprints for FBI criminal history (federal check) is required to advise applicants of the following PRIOR to submitting the fingerprint card for a criminal history check:
  - Applicants must be notified in writing that their fingerprints will be used to check the criminal history records of the FBI. The written notification to the applicant includes electronic notification.
  - Informing all applicants that they are allowed a reasonable opportunity (this must be defined in a tribal policy, i.e. 5 days) to complete and challenge the accuracy of their criminal history record before a final denial of a license and/or employment.
  - TGRAs must notify applicants in writing how to obtain a copy of the FBI record, how to update, correct, change, or challenge it, and that the guidelines for these procedures are contained in Title 28 C.F.R. § 16.34.

Additionally:

- The TGRA/tribe must also establish and document what constitutes a reasonable period of time for the review and challenge of the criminal history record and any appeals process that is available to the applicant.

- It is highly recommended (but not required) that the written notifications be presented to the applicant on a document that the applicant is required to sign.

### 5.2.3 Privacy and Security

TGRAs must have written policies and procedures regarding access, use, handling, dissemination, and destruction of CJI/CHRI (See Section 3.1). The NIGC Compliance Officer will review the TGRA/tribe's required privacy and security policies and procedures and any documents/processes related to security and dissemination of CJI/CHRI. Section 3 of this guide covers required policies and basic privacy and security guidelines.

- 1) The TGRA/tribe must have a process which ensures that CJI/CHRI is only used for the purpose for which it is requested. Under IGRA that purpose is licensing and/or employment of key employees and primary management officials of the tribe's gaming enterprise.
- 2) The TGRA/tribe must have processes in place for the proper access and handling of CJI/CHRI.
  - Access includes:
    - Defining who is authorized to access CJI/CHRI
    - Restricting access to only Authorized Personnel
  - Handling rules include:
    - Proper security of CJI/CHRI from receipt through destruction
    - Communication rules
      - Communication among Authorized Personnel
      - Communication with the applicant concerning CJI/CHRI
      - Communication with the NIGC upon discovery of security incidents (within 24 hours)
    - Secondary/Reuse dissemination procedures (if authorized by federal or state law beyond IGRA)
      - As a general matter, secondary dissemination or reuse is not allowed for CJI/CHRI obtained from the NIGC
      - Logging/tracking procedures
      - Procedures for authenticating recipients of the disseminated information
  - Retention procedures
  - Destruction procedures
- 3) The Tribe must have processes in place to prevent the unauthorized disclosure of CJI/CHRI. Prevention of unauthorized disclosure includes:
  - Access-limited storage.
  - Not leaving CJI/CHRI unattended when it is not physically secured.
  - Revocation of access privileges for terminated employees or those removed from the Authorized Personnel List.
- 4) The TGRA/tribe must have a formal disciplinary process in place for misuse of CJI/CHRI. This includes a formal sanctions process for personnel that fail to comply with information security policies and procedures, including those mandated by the CJIS Security Policy.
- 5) If applicable, the TGRA/tribe must have processes in place governing electronic storage of CJI/CHRI. This includes:
  - Monitoring and restricting access to databases containing CJI/CHRI.
  - Physical/technical safeguards to protect the access and integrity of the CJI/CHRI.
  - Reporting, response, and security incident handling capability for information security incidents.

#### **5.2.4 Training**

The NIGC Compliance Officer will review the TGRA/tribe's training documentation to verify Authorized Personnel have received both the mandatory CJIS training (or equivalent) and the TGRA/tribe's internal process training. All personnel with access are required to be trained in both.

- 1) All Authorized Personnel must be trained in the online security awareness (CJIS or equivalent) training within six months of hire or of being placed on the Authorized Personnel List and then every two years thereafter.
- 2) All Authorized Personnel must receive the TGRA/tribe's internal training on the access/use/handling/ dissemination/destruction procedures within six months of hire or of being placed on the Authorized Personnel List and then every two years thereafter. The Tribe's training must also cover the federal and tribal consequences for misuse of criminal history. The Compliance Officer will ask to view the TGRA/tribe's training and any reference policies to assess the training topics. (See Section 4.2.1)
- 3) All Authorized Personnel must sign an Acknowledgement Statement acknowledging the notification of the penalties for misuse of CJI/CHRI. There is no standard format for the Acknowledgement Statement, but it must state at a minimum that the individual has been notified of the consequences of misuse of CJI/CHRI. Agencies may choose to summarize the consequences on the Acknowledgement Statement or refer to specific policies or training materials. (See Section 4.2.2)
- 4) Authorized Personnel training must be logged on the NCJA Training Documentation Form (or equivalent) Specifically, the TGRA/tribe must document each instance when its Authorized Personnel receive training and retain documentation for a minimum of two years. The training documents must be available for inspection by FBI and NIGC auditors and Compliance Officers.

#### **5.2.5 Key Employee and Primary Management Official Checklist**

This checklist is provided to assist the TGRA/tribe in determining which gaming license or employment applicants' fingerprints can be submitted through the NIGC to obtain a CHRI for eligibility determinations. The checklist will be used by the NIGC during the audit process and the checklist or a similar process should be used by the TGRA/tribe to ensure only those employees who meet the definition of Key Employee and Primary Management official are fingerprinted through the NIGC. Tribal Gaming Commission staff and Gaming Commissioner are not typically employees of the gaming operation therefore they do not meet the definition of Key Employee or Primary Management Official listed below. For more information on the NIGC background and licensing regulations, please visit <https://www.nigc.gov/general-counsel/commission-regulations> parts 556 and 558.

#### **5.2.6 Gaming Operation Definition**

25 C.F.R. § 502.10 defines Gaming Operation as the economic entity that is licensed by a tribe, operates the games, receives the revenues, issues the prizes, and pay the expenses. A gaming operation may be operated by a tribe directly; by a management contractor; or, if individually-owned gaming is allowed, by another person or other entity.

#### **5.2.7 Key Employee Definition**

Per 25 C.F.R. §502.14 defines Key Employee as:

- (a) A person who performs one or more of the following functions:  
Bingo caller, counting room supervisor, Chief of Security, custodian of gaming supplies or cash, floor manager, pit boss, dealer, croupier, approver of credit, or custodian of gambling devices including persons with access to cash and

- accounting records within such devices;
- (b) If not otherwise included, any other person whose total cash compensation is in excess of \$50,000 per year; or,
- (c) If not otherwise included, the four most highly compensated persons in the gaming operation.
- (d) Any other person designated by the tribe as a key employee.

### 5.2.8 Primary Management Official Definition

Per 25 C.F.R. §502.19 defines Primary Management Official as:

- (a) The person having management responsibility for a management contract;
- (b) Any person who has authority:
  - (1) To hire and fire employees; or
  - (2) To set up working policy for the gaming operation; or
- (c) The chief financial officer or other person who has financial management responsibility.
- (d) Any other person designated by the tribe as a primary management official.

Any Key Employee or Primary Management Official who are classified under 25 C.F.R. 502.14 (d) and 502.19 (d) must have an attribute of 25 C.F.R 502.14 (a-c) or 502.19 (a-c)

A sample Key Employee and Primary Management Official checklist can be found in Appendix L.

Additionally, a Key Employee and Primary Management Official bulletin can be found in Appendix M.

When submitting a Notice of Results (NOR) to the NIGC, the document may contain summary CHRI if specifically referencing the FBI CHRI results. Updating the NOR to remove the FBI CHRI results can help eliminate summary CHRI. A revised sample NOR form can be found in Appendix N.

### 5.3 National Identity Services Audit

The FBI's CJIS Division has established audit programs for the purpose of evaluating compliance with policy requirements associated with access to CJIS systems and information. The National Identity Services (NIS) Audit assesses compliance with Interstate Identification Index (III) and National Fingerprint File (NFF) participation standards; federal laws and regulations associated with the use, dissemination, and security of national CHRI; and National Crime Prevention and Privacy Compact (Compact) rules and procedures. The NIS Audit is conducted with state criminal history record repositories, federal agencies, FBI-approved channelers, and other entities authorized access to Next Generation Identification (NGI) and III, and includes reviews of local agency components within their applicable jurisdictions.

Agencies which access criminal history records for non-criminal justice licensing and employment purposes must meet requirements established in federal laws and regulations, as well as requirements established by the Compact Council for such access. Specific policies include: Use of CHRI; Reason Fingerprinted Field and Purpose Code Usage; Dissemination of CHRI; Applicant Notification and Record Challenge; Name-Based III Access Using Purpose Codes I and X; User Fee; and Audit Program. Primary sources for these policy requirements include:

- Title 28, U.S.C Section 534 (a)(4) and (b)
- Title 42, U.S.C, Section 14616, Article IV (c) and Article V (a) and (c)
- Title 5, U.S.C., Section 552a, (e)(3)
- Title 28, C.F.R. Section 50.12, (b)
- Title 28, C.F.R., Section 20.33, (a)(3) and (d) • Title 28, C.F.R., Section 901

- III/NFF Operational and Technical Manual, Chapter 2, Section 2
- CJIS Security Policy, Version 5.3, Section 5.11.2

For more information on the NIS Audit, please visit <https://www.fbi.gov/file-repository/national-identity-services-pdf.pdf/view>

## **5.4 Information Technology Security Audit**

The purpose of the audit is to assess the user community's compliance with the FBI CJIS Security Policy requirements as approved by the Advisory Policy Board (APB) and National Crime Prevention and Privacy Compact (Compact) Council. The FBI CJIS Security Policy provides a baseline of security requirements for current and planned services and sets a minimum standard for new initiatives. The FBI CJIS Security Policy applies to all entities with access to, or who operate in support of, FBI CJIS Division's services and information. The FBI CJIS Security Policy provides the minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, and/or destruction of CJI and CHRI. Entities engaged in the interstate exchange of CJI/CHRI data for non-criminal justice purposes are also governed by the standards and rules promulgated by the Compact Council to include the Outsourcing Standard for Nonchannelers.

**5.4.1 Noncriminal Justice Audit** - an audit of a non-criminal justice agency's access, use, storage, and destruction of any CJI/CHRI received from FBI CJIS systems via direct and indirect access methods. These audits include both name-based and fingerprint-based queries over wired or wireless networks.

**5.4.2 Outsourcing/Channeling Audit** – an audit of an FBI approved contractor who submits fingerprints on behalf of an authorized recipient to the FBI and receives the results of such a submission for dissemination back to the authorized recipient. The scope of nonchanneler audits focuses mainly on the storage, dissemination, and destruction of CHRI.

These audits are comprised of an administrative interview to review administrative and technical controls that are implemented to protect CJI/CHRI from both a physical and logical perspective. Additionally, most audits include a physical security and network inspection in which controls identified in the administrative interview are verified to be implemented and working correctly. For more information on the Information Technology Security Audit please visit <https://www.fbi.gov/file-repository/information-technology-security.pdf/view>

## Section 6 – NIGC Classes & Assistance

The NIGC provides training to noncriminal justice agencies receiving CJI and CHRI. The NIGC's compliance training is designed to help the Local Agency Security Officer (LASO) or other designated tribal representatives understand the compliance requirements so that they can implement the rules back at their Tribe. The NIGC training **does not** take the place of the TGRA/tribe's internal training. It is each TGRA/tribe's responsibility to ensure that its Authorized Personnel are properly trained in the requirements detailed in Section 5.2.4.

### 6.1 Initial Access & NCJA Compliance Training

All new TGRAs are required to have at least one representative complete Initial Access & NCJA Compliance Training prior to submitting any fingerprint cards. This training is not required for existing TGRAs; however, it is recommended if a TGRA/tribe has experienced personnel turnover or TGRA/tribal personnel wish to attend a refresher in order to ensure compliance with current requirements. The persons who attend training should be prepared to share the information learned with other relevant TGRA/tribal personnel. This training is for the LASO and tribal trainers – this is NOT the training which is required for all Tribe Authorized Personnel. Authorized Personnel training requirements are explained in the class.

#### *Class Description*

Initial Access & NCJA Compliance Training lasts approximately six hours and covers the basic rules in this guide and provides information on the following:

- How to properly fill out the information on a fingerprint card.
- Fingerprint submission packet requirements
- How to read and interpret CJI/CHRI.
- Complying with NIGC and federal requirements associated with noncriminal justice fingerprint criminal history checks
- The LASO's role as the primary TGRA/tribal liaison and guidance regarding TGRA/tribal regulatory compliance and required documentation.
- Basic privacy and security guidelines for the access, use, handling, and destruction of criminal history record information.
- The key areas the TGRAs need to consider when developing policies and procedures for criminal history handling.
- How to identify Key Employees and Primary Management Officials of tribal gaming enterprises.
- Authorized personnel training requirements and an overview of CJIS Online Security Awareness training.
- How to achieve compliance with the FBI and NIGC requirements.

### 6.2 Types of Training Offered by the NIGC

The NIGC offers several methods for completing the Initial Access & NCJA Compliance Training. Trainings will be provided at Regional Training Course (RTC) locations yearly as well as offered as Site Specific Training (SST). Additional resources may be located on the NIGC website at <https://www.nigc.gov/compliance/CJIS-Training-Materials>.

### 6.3 Requesting Site Specific Training from the NIGC

Site Specific training is offered to the TGRA and tribe at no cost and can be provided by NIGC Regional staff. To request Site Specific Training please complete the training request form located at <https://www.nigc.gov/training/>. NIGC Region staff will work with the Tribe to schedule and provide the training.

## **6.4 Other Training Options**

The TGRA/tribe can develop and utilize their own security awareness training instead of completing the NIGC training to ensure compliance. The NIGC and FBI allow multiple options to meet the training requirements.

## Section 7 - First Steps to Achieve Compliance

### 7.1 How to achieve compliance

The NIGC has created the following guideline to assist TGRAs in ensuring compliance with the FBI CJIS Security Policy and NIGC MOU requirements.

1. Review Memorandum of Understanding with NIGC (10 days)
  - a. Ensure most recent version is in use (current version 2017);
  - b. Ensure current TGRA head or authorized official has executed agreement; and
  - c. Ensure all staff subject to agreement and using CHRICHRICHI has reviewed its contents.
2. Update authorized personnel list (<http://bit.ly/AUserList>): (10 days)
  - a. Designate Local Agency Security Officer (LASO);
  - b. List all personnel with access to FBI CHRI received from NIGC; and
  - c. Send authorized personnel list to NIGC Information Security Officer (ISO) at [iso@nigc.gov](mailto:iso@nigc.gov)...
  - d. Maintain up-to-date authorized personnel list on site and on record with NIGC ISO.
3. Complete and document initial CJIS Security Awareness Training within next 6 months via (30 -60 days):
  - a. PowerPoint presentation;
  - b. Video presentation; or
  - c. Online.
4. Begin reviewing resource information (<https://www.nigc.gov/compliance/CJIS-Training-Materials>) (30-60 days):
  - a. National Information Systems (NIS) Resource Guide;
  - b. Criminal Justice Information Services (CJIS) Security Policy
  - c. NIGC Fingerprint site (<https://www.nigc.gov/finance/fingerprint-process>); and
  - d. TGRA internal policies.
5. Complete CJIS IT Questionnaire (<http://bit.ly/CJISITQuestions>) (10 days):
  - a. Determine readiness/compliance level; and
  - b. Begin improving network hardware, software and policy to achieve compliance (6-12 months).
6. Develop/refine written internal TGRA policies to meet CJIS requirements including (6-12) months:
  - a. Use of fingerprint based CHRI;
  - b. Applicants Rights Notice/FBI Privacy Act Notice/Opportunity to Correct/Copy of CHRI;
  - c. Security Awareness Training;
  - d. Incident Response Policy;
  - e. Auditing and Accountability;
  - f. Access Control;
  - g. Identification and Authentication;
  - h. Configuration Management;
  - i. Media Protection;
  - j. Physical Protection;
  - k. System and Communication Protection and Information Integrity;
  - l. Formal Audits;
  - m. Personnel Security; and
  - n. Mobile Devices;
7. Complete and document internal training on TGRA policies (following timeline of Step 6, 30-60 days).
8. Authorized personnel sign training/penalty acknowledgement statements for TGRA policies (following Step 7).

9. Outsourcing Agreements for non-channelers (6-9 months):
  - a. Identify all IT service providers with access to electronic media containing unencrypted FBI CHRI;
  - b. Identify other service providers with unescorted access to physical copies of CHRI (shredding services, storage facilities);
  - c. Submit request letter to FBI Compact Officer for outsourcing contract approval;
  - d. Execute contract;
  - e. Complete 90-day audit of contractor; and
  - f. Provide certification to FBI Compact Officer that contractor meets CJIS Security Policy.
10. Prepare for first annual NIGC audit using site visit checklist (<http://bit.ly/CJISSVCKList>) (on-going).
11. Continue internal auditing/monitoring to maintain compliance with FBI requirements (on-going).
12. Complete biennial training for users and annually for outsourced non-channelers (on-going).

FBI CJIS Auditor will select three to four tribes Summer/Fall of 2021 for testing against full compliance with NIS and CJIS Security Policy standards as they apply to non-criminal justice agencies and the NIGC MOU.

## References

The following state and federal sources referenced below contain rules, regulations, and policies governing the use and dissemination of CJI and CHRI for noncriminal justice purposes. Most of these sources can be readily accessed online. This list is not exhaustive. Additional rules may also be contained in the specific authorization which allows the TGRA/tribe to access CJI/CHRI.

### Federal References

U.S. Code of Federal Regulations:

<https://www.gpo.gov/fdsys/browse/collectionCfr.action?collectionCode=CFR>

- Title 28 C.F.R. 20 - Subpart C Federal System and Interstate Exchange of Criminal History Record Information
- Title 28 C.F.R. 0.85(j) - FBI authorized to approve procedures relating to the exchange of identification records.
- Title 28 C.F.R. 50.12 - Funds/approval for records exchange; dissemination limitations; required notification; review and challenge

United States Code: <http://uscode.house.gov/search/criteria.shtml>

- Title 5 U.S.C. 552 - Freedom of Information Act
- Title 5 U.S.C. 552a - Privacy Act of 1974 (as amended)
- Title 42 U.S.C. 14616 - Compact Council

Federal Bureau of Investigation: <https://www.fbi.gov>

- National Crime Prevention and Privacy Compact Council Compact Council Library: Resource documents and references by the Compact Council.
- Identity Verification Program Guide: Published by the National Crime Prevention and Privacy Compact Council to aid fingerprint-submitting agencies in developing policy, procedures, and practices for positive identification of applicants.
- Federal Bureau of Investigations Criminal Justice Information Services (CJIS), CJIS Security Policy.

## Acronym Glossary

3DES	Triple Data Encryption Standard
AFIS	Automated Fingerprint Identification System
ASCII	American Standard Code for Information Interchange
CHRI	Criminal History Record Information
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
CRI	Contributor Agency Identifier
CSA	CJIS Systems Agency
CSO	CJIS Systems Officer
CTA	Central Terminal Agency
DAI	Designation Agency Identifier
DES	Data Encryption Standard
EFTS	Electronic Fingerprint Transmission Specification
ERRT	Ten-print Transaction Error
ESP	IP Encapsulating Payload
FAUF	Federal Applicant User Fee
FBI	Federal Bureau of Investigation
IAFIS	Integrated Automated Fingerprint Identification System (FBI)
IKE	Internet Key Exchange
IPSec	Internet Protocol Security
IT	Information Technology
L2TP	Layer Two Tunneling Protocol
LASO	Local Agency Security Officer
MIME	Multipurpose Internet Mail Extensions
MOU	Memorandum of Understanding
MS-CHAP	Microsoft PPP Challenge Handshake Authentication Protocol
NCIC	National Crime Information Center
NCJA	Noncriminal Justice Agency
NIGC	National Indian Gaming Commission
NIST	National Institute of Standards and Technology
OCA	Originating Agency Case Number
ORI	Originating Agency Identifier
PII	Personal Identification Information
POP3	Post Office Protocol (version 3)
PPTP	Point-to-Point Tunneling Protocol
RTC	Regional Training Course
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transport Protocol
SnF	NIGC's Fingerprint Store and Forward Server
SRE	Submission Results — Electronic
SST	Site Specific Training
TCN	Transaction Control Number
TCP/IP	Transmission Control Protocol / Internet Protocol
TCR	Transmission Control Reference
TOT	Type of Transaction

# Appendix A

## MEMORANDUM OF UNDERSTANDING BETWEEN THE FEDERAL BUREAU OF INVESTIGATION AND NATIONAL INDIAN GAMING COMMISSION CONCERNING NONCRIMINAL JUSTICE FINGERPRINT SUBMISSIONS

### I. PURPOSE

This Memorandum of Understanding (MOU) documents the agreed-upon responsibilities and functions of the parties with respect to the submission of noncriminal justice fingerprints for primary management officials and key employees of Indian **gaming enterprises**, as defined by NIGC regulations, **25 C.F.R. §§ 502.14(a-c) and 502.19(a-c)**.

### II. PARTIES

This MOU is between the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division, and the National Indian Gaming Commission (NIGC), hereinafter referred to as "Parties".

### III. AUTHORITIES

The FBI enters into this MOU under the authority of **28 U.S.C. § 534**. The NIGC enters into this MOU under the NIGC's fingerprint collection and background check authorities that include the following: **25 U.S.C. §§ 2706(b)(3), 2706(b)(7), 2706(b)(10), 2708, 2710(b)(2)(F), 2710(c)(1)-(2), 2710(d)(9), 2711(a), 2711(e)**.

### IV. BACKGROUND INFORMATION

The Indian Gaming Regulatory Act (IGRA) established federal standards for gaming on Indian lands to protect Indian gaming as a means of generating tribal revenue. 25 U.S.C. § 2702(3). To carry out this purpose, Congress generally authorized the NIGC to "conduct or cause to be conducted such background investigations as may be necessary" and to "promulgate regulations and guidelines as it deems appropriate to implement the provisions of the IGRA. *Id.* § 2706(b)(3), (10). To assist in that role, Congress specifically provided the NIGC with the power to "secure from any department or agency of the United States information necessary to enable it to carry out" those functions. *Id.* § 2708.

The NIGC submits fingerprints of key employees and primary management officials of Indian gaming enterprises as part of the background screening process required by IGA. *See* 25 U.S.C. § 2710(b)(2)(F), (c)(1)-(2), & (d)(1)(A). The NIGC also submits fingerprints and performs background investigations of "each person or entity ... having a direct financial interest in, or management responsibility for" a management contract. *Id.* § 2711(a). The authority to receive criminal history information for key employees and primary management officials of class II and class III gaming enterprises stems from statutory language specifically empowering the NIGC Chair to "consult with appropriate law enforcement officials concerning gaming licenses issued by an Indian tribe" and to facilitate the suspension of gaming licenses when a key employee or primary management official does not meet the statute's suitability standards with regard to an applicant's criminal history. 25 U.S.C. § 2710(b)(2)(F)(ii)(II), (c)(1)-(2), (d)(1)(A)(ii). Likewise, § 2711(e) requires the Chairman to review the criminal history information of persons with a direct or indirect financial interest in management contracts and to disapprove a management contract when one of those individuals "has been or subsequently is convicted of any felony or gaming offense" or where his or her "criminal record if any ... pose[s] a threat to the public interest or to the effective regulation and control of gaming." This, likewise, applies to both class II and class III gaming. *See* 25 U.S.C. § 2711(e)(1)(B); 25 C.F.R. § 533.6(b)(1)(ii), (c).

### V. SPECIFIC RESPONSIBILITIES

#### A. The FBI will:

1. Conduct fingerprint-based criminal history record searches of NIGC submissions and return the results of the checks to the NIGC.
2. Return rejected fingerprint submissions to NIGC. The NIGC is responsible for notifying each subject of deficiencies in the fingerprint submissions that were rejected by the FBI.
3. Bill NIGC for fingerprint submissions in accordance with the terms of the Interagency Agreement between the NIGC and the CJIS Division.
4. Ensure that the NIGC is not charged supplemental fees for resubmissions and reprocessing of illegible (i.e., unclassifiable) fingerprints, provided that the NIGC follows the procedures outlined by the CJIS Division for the resubmission of the fingerprint cards returned to the NIGC. (This waiver is limited to one resubmission per subject.)

#### B. The NIGC will:

1. Ensure that all fingerprint submissions have been properly and adequately completed.
2. Convert properly submitted fingerprint card submissions into an electronic format and forward them to the FBI via a means acceptable to the FBI.

3. Collect and remit the FBI's fee for the processing of the applicant fingerprint submission. (See 83 FR 48335, dated September 24, 2018, or any successor fee schedule.)

VI. EFFECT OF THIS AGREEMENT

- A. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise against any of the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof. The parties will seek to resolve any disputes regarding this MOU by mutual consideration.
- B. Except as provided in this document, this MOU is not an obligation or commitment of funds, nor a basis for the transfer of funds, but rather is a basic statement of the understanding between the Parties of the matters described herein. Unless otherwise agreed in writing, each Party shall bear its own costs in relation to this MOU. Expenditures by each Party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that the language in this MOU in no way implies that funds will be made available for such expenditures.
- C. This MOU does not constitute an agreement for any Party to assume or waive any liability or claim under any applicable law.
- D. The information involved in this MOU may identify U.S. persons, whose information is protected by the Privacy Act of 1974 and/or Executive Order 12333 (or any successor executive order). All such information will be handled lawfully pursuant to the provisions thereof.
- E. Each Party will only disclose personally identifiable information (PII) as authorized under applicable system of records notices published in the Federal Register. For purposes of this MOU, PII is defined as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric information, etc., including any other personal information which is linked or linkable to a specific individual."
- F. Before using PII shared pursuant to this MOU, the recipient agency will make reasonable efforts to ensure that the information is accurate, timely, relevant, and complete.
- G. In the event that either Party to this MOU becomes aware of any inaccuracies in the information received from the other Party pursuant to this MOU, the information recipient will promptly notify the information provider so that corrective action can be taken.
- H. Each Party will immediately report to the other Party each instance in which information received from the other Party is used, disclosed, or accessed in an unauthorized manner (including any information losses or breaches).
- I. Each Party will provide appropriate training regarding the responsibilities under this MOU to individuals whose information sharing activities are covered by the provisions of this MOU.
- J. Subject to federal law or regulation, either Party or both Parties may audit the handling and maintenance of information relevant to this MOU in electronic and paper recordkeeping systems to ensure that appropriate security and privacy protections are in place.

VII. EFFECTIVE DATE, MODIFICATION AND TERMINATION

This agreement shall be effective when executed by both Parties and will continue in effect until terminated. This agreement may be modified at any time by written consent of both Parties.

This MOU may be terminated with respect to any Party, at any time, upon written notice of withdrawal to the other Party. Any Party desiring to terminate or modify this MOU will provide such written notification to the other Party at least thirty (30) days prior to modification or termination. The Parties intend to review this MOU annually to ensure all provisions are meaningful and current.

**The preceding seven sections represent the understanding reached by the Parties.**

**FEDERAL BUREAU OF INVESTIGATION,**

  
Michael D. DeLeon  
Assistant Director

2/10/2020

Date

**Criminal Justice Information Services Division**

**NATIONAL INDIAN GAMING COMMISSION.**



1/17/2020  
Date

**Christinia J. Thomas Acting Chief of Staff**

**National Indian Gaming Commission**

**MEMORANDUM OF UNDERSTANDING  
REGARDING THE DISSEMINATION OF CRIMINAL HISTORY RECORD  
INFORMATION BY THE NATIONAL INDIAN GAMING COMMISSION**

In order to facilitate the undersigned tribe (Tribe) in determining the suitability of individuals who have applied for positions as key employees or primary management officials in its gaming operation(s), the National Indian Gaming Commission (NIGC) will be obtaining criminal history record information (CHRI) from the Federal Bureau of Investigation (FBI) on these individuals and disseminating such information to the Tribe.

This memorandum sets forth the following conditions under which the NIGC will disseminate the CHRI to the Tribe:

1. Prior to taking an applicant's fingerprints, the Tribe agrees to provide the applicant with a written notification that informs the applicant that: (i) his or her fingerprints will be used to check the criminal history records maintained by the FBI; (ii) he or she has the opportunity to complete or challenge the accuracy of the information contained in the FBI identification record; (iii) the procedures for obtaining a copy of his or her FBI criminal history record are set forth at 28 CFR §§ 16.30 - 16.33, or by visiting the FBI's website at <<http://www.fbi.gov/about-us/cjis/background-checks>>; and (iv) the procedure for obtaining a change, correction, or updating an FBI identification record are set forth at 28 CFR § 16.34. The Tribe understands that if it does not provide the applicant with this written notification, the NIGC will not disseminate the CHRI to the Tribe.
2. The Tribe understands that the FBI has retained the right to approve the dissemination of the CHRI and may, at some future date, prohibit the NIGC from disseminating CHRI. The Tribe further understands that the NIGC will not release any CHRI without first having received all required prior approvals from the FBI and will not release any CHRI when prohibited from doing so by the FBI. The Tribe also understands that the FBI may impose additional restrictions on the dissemination and use of the CHRI (in addition to those imposed by the NIGC), and that the Tribe will be subject to all such additional restrictions.
3. The Tribe agrees that any CHRI disseminated by the NIGC may be used by the Tribe solely for the purpose of determining a particular applicant's suitability for employment in the Tribe's gaming operation(s).
4. The Tribe understands that NIGC disseminations will only contain the CHRI on a particular applicant and will not contain any NIGC recommendations or conclusions. However, the NIGC reserves the right to furnish (to the Tribe) summary memoranda containing the results of the CHRI.
5. The Tribe agrees that any and all CHRI with which it is provided shall be afforded proper security. The Tribe shall ensure that access to all CHRI disseminated by the NIGC, including all summary memoranda, is restricted to tribal personnel directly involved in licensing deliberations. The Tribe agrees to maintain records of the identities of all persons having access to the CHRI and such records shall be furnished to the NIGC upon request.
6. The Tribe agrees that, except in connection with proceedings related to the Tribe's licensing determinations for its gaming employees, neither the CHRI nor any summary memoranda disseminated by the NIGC shall be reproduced, distributed, or introduced in a court of law or administrative hearing, without the NIGC's prior written consent.
7. The NIGC agrees to promptly notify tribal authorities in the event that the NIGC determines that it is necessary to discontinue disseminating CHRI to the Tribe (either in whole or in part) due to the Tribe's failure to comply with the conditions set forth in this memorandum.

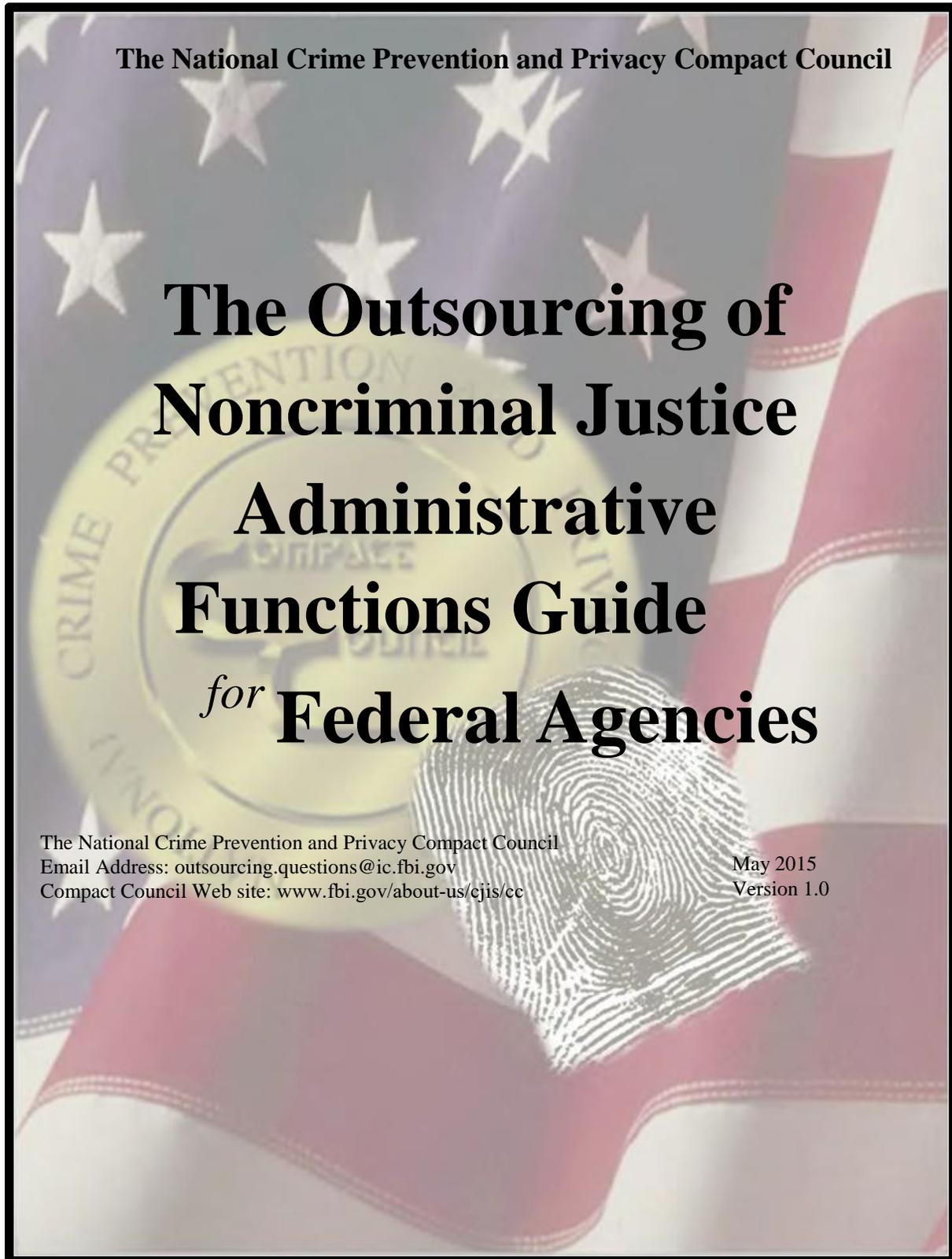
The Tribe acknowledges and consents to the above-stated conditions on this \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_.

\_\_\_\_\_  
Name of Tribe

\_\_\_\_\_  
Name of Authorized Tribal Official (PRINT)

## Appendix B

The following items are only a select few pages from the full Outsourcing Guide. For the full guide please visit <https://www.nigc.gov/compliance/CJIS-Training-Materials>. Additionally, the Compact Council may update the standards from time to time. Please check with the FBI Compact Officer for most recent guide.



**The National Crime Prevention and Privacy Compact Council**

# **The Outsourcing of Noncriminal Justice Administrative Functions Guide *for* Federal Agencies**

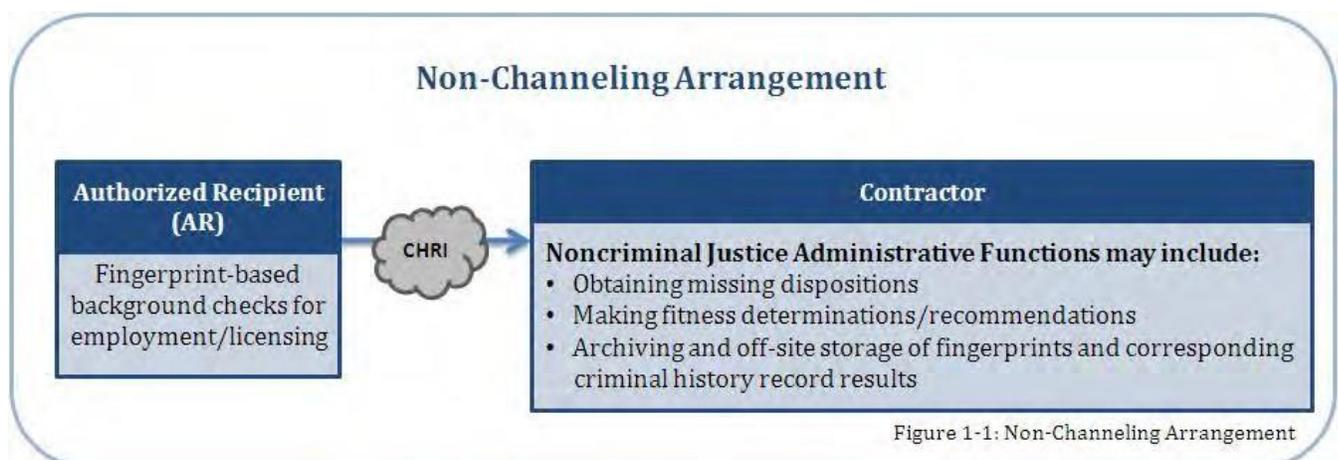
The National Crime Prevention and Privacy Compact Council  
Email Address: [outsourcing.questions@ic.fbi.gov](mailto:outsourcing.questions@ic.fbi.gov)  
Compact Council Web site: [www.fbi.gov/about-us/cjis/cc](http://www.fbi.gov/about-us/cjis/cc)

May 2015  
Version 1.0

## Outsourcing: Non-Channeling versus Channeling

There are two very separate and distinct parts to the outsourcing of noncriminal justice administrative functions associated with national criminal history records. The first is Non-Channeling. In this scenario, the Contractor receives access to the CHRI directly from the AR. The AR may engage the Contractor to perform a variety of noncriminal justice administrative functions, such as, but not limited to, obtaining missing dispositions, making fitness determinations/ recommendations, or the off-site storage and archival of fingerprint submissions and corresponding criminal history record results. In this arrangement, the Contractors do not have a direct connection to the FBI's CJIS Wide Area Network (WAN). The AR provides the results of the national criminal history record check directly to the Contractor. The Contractor performs the desired noncriminal justice administrative function(s). Figure 1-1 depicts a Non-Channeling arrangement.

It is important to note that in order to fully comply with footnote 4 of the Outsourcing Standard for Non-Channelers, which provides that if a national criminal history record check of government personnel having access to CHRI is mandated or authorized by a federal statute or executive order approved by the U.S. AG, then the AR must ensure Contractor personnel accessing CHRI are either covered by existing law or that the existing law be amended to include national criminal history record checks for Contractors prior to authorizing the outsourcing initiatives.



The other part of noncriminal justice outsourcing is Channeling, which creates a conduit for an AR to submit fingerprints via an FBI-approved Channeler directly to the FBI, the Channeler receives the CHRI on behalf of the AR, and promptly distributes the CHRI to the AR. The Channeler is a Contractor that has a direct connection to the FBI's CJIS WAN for the electronic submission of fingerprints on behalf of the AR. The FBI electronically returns the corresponding results of each fingerprint-based national criminal history record check to the Channeler and the Channeler expeditiously disseminates the criminal history record check results to the AR. Figure 1-2 illustrates the Channeling arrangement.

In 2011, the FBI released a Request for Proposal (RFP) to solicit Contractors to provide processing services for authorized national noncriminal justice fingerprint submissions from ARs. In response to the RFP, the FBI selected multiple Contractors to act as Channelers. For a current list of Channelers, visit <[www.fbi.gov/about-us/cjis/cc/current-initiatives/list-of-fbi-approved-channelers](http://www.fbi.gov/about-us/cjis/cc/current-initiatives/list-of-fbi-approved-channelers)> or contact the FBI Compact Office at <[outsourcing.questions@ic.fbi.gov](mailto:outsourcing.questions@ic.fbi.gov)>. Pursuant to the Outsourcing Standard for Channelers, the FBI is required to conduct criminal history record checks of Channeling personnel having access to CHRI. Thus, in this arrangement, the AR is not responsible for conducting background checks of the Contractor's personnel having access to CHRI.

As a matter of information, if the Contractor is posting national criminal history record check results to a Web site, the FBI CJIS Division's Information Security Officer must review and approve the proposed technical configuration prior to the FBI Compact Officer's decision to approve the request.

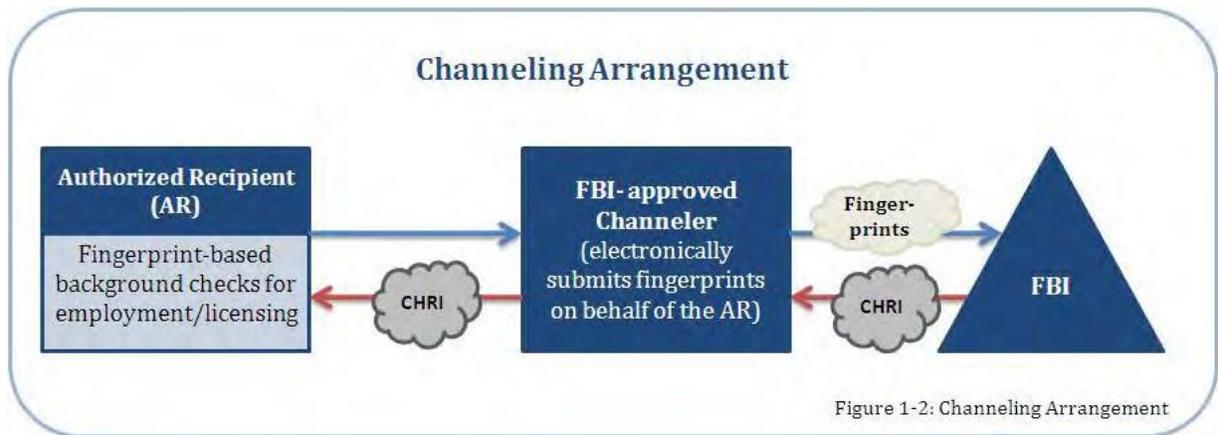


Figure 1-2: Channeling Arrangement

It is possible for the same Contractor to provide both Channeling and Non-Channeling noncriminal justice administrative function services. If this occurs, there must be a distinct separation between the Channeling and the performance of the other noncriminal justice administrative functions (Non-Channeling). A Channeler must promptly forward the criminal history record check results to the AR, which ends the "Channeling" outsourcing process. Then, the AR would be responsible for selecting and forwarding the criminal history record check results back to the Contractor for the performance of approved Non-Channeling noncriminal justice administrative functions, such as obtaining missing dispositions, outsourced by the AR in compliance with the Outsourcing Standard

for Non-Channelers. Such procedures will establish a distinct beginning and end to each of the outsourcing contracts (i.e., a contract for Channeling and a contract for other noncriminal justice administrative functions). Additionally, this process will facilitate an efficient audit process. Essentially, a Channeler is an “expediter” or “conduit” rather than a user of criminal history record results. The Contractor providing the Non-Channeling function is the user of the information. Figure 1-3 displays the same Contractor performing both the Channeling and Non-Channeling functions.

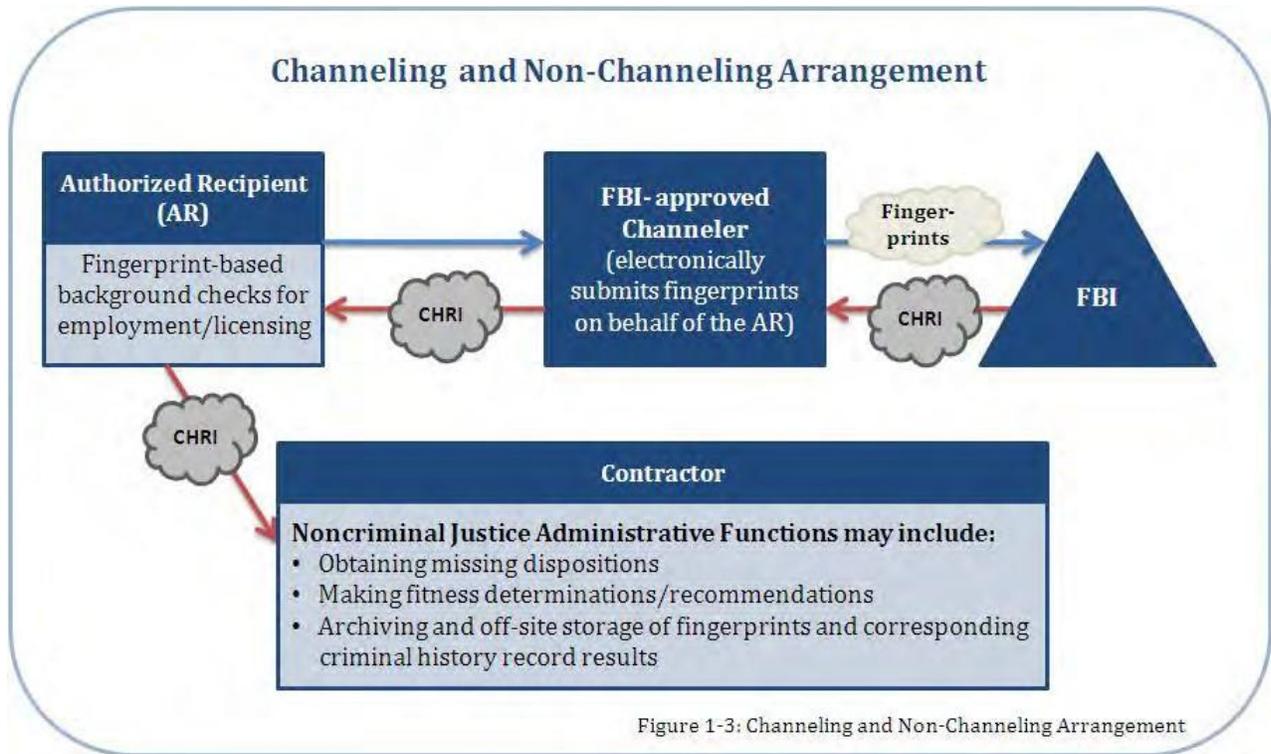


Figure 1-3: Channeling and Non-Channeling Arrangement

## **Authorized Recipient's Responsibilities**

---

Prior to engaging in the outsourcing of any noncriminal justice administrative functions, the AR is required to request and receive written permission from the FBI Compact Officer. The following sections provide examples of Non-Channeling and Channeling documentation and may be used as a reference when drafting documents relating to the outsourcing of noncriminal justice administrative functions.

### **Non-Channeling Sample Documentation**

- Authorized Recipient Sample Request Letter for Non-Channeling
- Authorized Recipient Sample FBI Response Letter for Non-Channeling
- Sample Language between the Authorized Recipient and Contractor regarding Noncriminal Justice Outsourcing Functions for Non-Channeling

## Examples of Non- Channeling Documentation

REQUEST LETTER  
FOR THE (Name) **TRIBAL GAMING COMMISSION** TO USE  
(Name) **TRIBAL IT DEPARTMENT** AS A CONTRACTOR  
FOR NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS

April 3, 2020

Mrs. Chasity S. Anderson  
Compact Officer, FBI Module D3  
1000 Custer Hollow Road  
Clarksburg, WV 26306

Dear Mrs. Anderson:

The (Name) **Tribal Gaming Commission**, the Authorized Recipient, requests permission to use the (Tribe) **Tribal IT Department** as a contractor to outsource noncriminal justice administrative functions relating to the processing of criminal history record information (CHRI) on its behalf. This would include **[insert all functions that may apply. For example, obtaining missing dispositions, making determinations and recommendations, off-site storage of criminal history record information and its corresponding fingerprint submissions, etc.]** The (Tribe) **Tribal Gaming Commission** and the (Tribe) **Tribal IT Department** are considering entering into an agreement in which (Tribe) **Tribal IT Department** will act on the (Tribe) **Tribal Gaming Commission's** behalf in accordance with the Security and Management Control Outsourcing Standard (Outsourcing Standard) for Non-Channelers. The (Tribe) **Tribal Gaming Commission** is authorized to perform background checks pursuant to Title 25, United States Code (U.S.C.), §2701, et seq, also referred to as the "Indian Gaming Regulatory Act (IGRA)." Specifically, the National Indian Gaming Commission (NIGC) is authorized to submit fingerprints to the FBI on behalf of the (Tribe) **Tribal Gaming Commission** for Class II and III primary management officials and key employees of the Tribal gaming enterprises. "Key employee" and "primary management official" are defined in Title 25, Code of Federal Regulations (C.F.R.), §§502.14 and 502.19 respectively.

The (Tribe) **Tribal Gaming Commission** will execute a contractual agreement with the Contractor, incorporating by reference the Outsourcing Standard for Non-Channelers and the Criminal Justice Information Services (CJIS) Security Policy. Execution of the agreement will commence upon receiving written approval from the FBI Compact Officer and, upon request from the FBI Compact Officer, receipt of a copy of the executed agreement. **The Authorized Recipient shall certify to the FBI Compact Officer that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.**

If for any reason the agreement is terminated by either the Authorized Recipient or the Contractor, the Authorized Recipient will provide written notification to the FBI Compact Officer as soon as possible. All records of the Authorized Recipient held by the Contractor will be returned or destroyed, in accordance with the Outsourcing Standard and the CJIS Security Policy, and employees of the Contractor will no longer be allowed access to the CHRI records of the Authorized Recipients.

Upon execution of the Contract, the (Tribe) **Tribal Gaming Commission** will take responsibility for (Tribe) **Tribal IT Department** compliance with the terms of the Contract, to include the Outsourcing Standard for Non-Channelers, and will notify the FBI Compact Officer of any violations.

Sincerely,

[insert name]  
[insert title]  
[insert address]  
[insert phone number]  
[insert email address]

cc: [iso@nigc.gov](mailto:iso@nigc.gov)

REQUEST LETTER  
FOR THE (Name) **TRIBAL GAMING COMMISSION** TO USE  
**(Contractor's Name)** AS A CONTRACTOR  
FOR NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS

April 3, 2020

Mrs. Chasity S. Anderson  
Compact Officer, FBI Module D3  
1000 Custer Hollow Road  
Clarksburg, WV 26306

Dear Mrs. Anderson:

The (Name) **Tribal Gaming Commission**, the Authorized Recipient, requests permission to use the **(Contractor's Name)** as a contractor to outsource noncriminal justice administrative functions relating to the processing of criminal history record information (CHRI) on its behalf. This would include **[insert all functions that may apply. For example, obtaining missing dispositions, making determinations and recommendations, off-site storage of criminal history record information and its corresponding fingerprint submissions, etc.]** The **(Tribe) Tribal Gaming Commission** and the **(Contractor's Name)** are considering entering into an agreement in which **(Contractor's Name)** will act on the **(Tribe) Tribal Gaming Commission's** behalf in accordance with the Security and Management Control Outsourcing Standard (Outsourcing Standard) for Non-Channelers. The **(Tribe) Tribal Gaming Commission** is authorized to perform background checks pursuant to Title 25, United States Code (U.S.C.), §2701, et seq, also referred to as the "Indian Gaming Regulatory Act (IGRA)." Specifically, the National Indian Gaming Commission (NIGC) is authorized to submit fingerprints to the FBI on behalf of the **(Tribe) Tribal Gaming Commission** for Class II and III primary management officials and key employees of the Tribal gaming enterprises. "Key employee" and "primary management official" are defined in Title 25, Code of Federal Regulations (C.F.R.), §§502.14 and 502.19 respectively.

The **(Tribe) Tribal Gaming Commission** will execute a contractual agreement with the Contractor, incorporating by reference the Outsourcing Standard for Non-Channelers and the Criminal Justice Information Services (CJIS) Security Policy. Execution of the agreement will commence upon receiving written approval from the FBI Compact Officer and, upon request from the FBI Compact Officer, receipt of a copy of the executed agreement. **The Authorized Recipient shall certify to the FBI Compact Officer that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.**

If for any reason the agreement is terminated by either the Authorized Recipient or the Contractor, the Authorized Recipient will provide written notification to the FBI Compact Officer as soon as possible. All records of the Authorized Recipient held by the Contractor will be returned or destroyed, in accordance with the Outsourcing Standard and the CJIS Security Policy, and employees of the Contractor will no longer be allowed access to the CHRI records of the Authorized Recipients.

Upon execution of the Contract, the **(Tribe) Tribal Gaming Commission** will take responsibility for **(Contractor's Name)** compliance with the terms of the Contract, to include the Outsourcing Standard for Non-Channelers, and will notify the FBI Compact Officer of any violations.

Sincerely,

**[insert name]**  
**[insert title]**  
**[insert address]**  
**[insert phone number]**  
**[insert email address]**

cc: iso@nigc.gov

## *Authorized Recipient Sample FBI Response Letter for Non-Channeling*

[Date]

[Name] [Position  
Title] [Division]  
[Federal Agency]  
[Address]  
[City, State and Zip Code]

Dear [Name]:

Reference is made to your request to use **[insert Contractor's name]** to perform the noncriminal justice administrative functions relating to the processing of criminal history record information (CHRI). This would be limited to **[insert specific noncriminal justice administrative functions to be performed]**. It is noted that your authority for access to the FBI CHRI is **[insert the legal citation of the federal statutory authority or executive order that requires or authorizes the Authorized Recipient to have access to CHRI]**.

In accordance with the National Crime Prevention and Privacy Compact Council's Final Rule entitled "Outsourcing of Noncriminal Justice Administrative Functions," (Title 28, Code of Federal Regulations, Part 906), outsourcing of noncriminal justice administrative functions is permitted under certain conditions when approved by the FBI Compact Officer and as specified in the Security and Management Control Outsourcing Standard for Non-Channelers (Outsourcing Standard).

The **[insert Authorized Recipient's name]** is granted permission to provide CHRI to **[insert Contractor's name]**, as its contractor, solely for the purpose of **[insert specific noncriminal justice administrative functions to be performed]** pursuant to this approval.

In the event of a conflict between the terms of the **[insert Authorized Recipient's name]/[insert Contractor's name]** agreement, amendments to the **[insert Authorized Recipient's name]/[insert Contractor's name]** agreement, and the Outsourcing Standard relating to FBI-provided data, the terms of the Outsourcing Standard shall control.

According to Part 2.05 of the Outsourcing Standard, **[insert Authorized Recipient's name]** shall conduct an audit of the contractor within 90 days of the date the contractor first receives CHRI under the approved outsourcing agreement and shall certify to me that the audit was conducted.

Further, as provided in footnote 2 of the Outsourcing Standard, the FBI will triennially audit a representative sample of contractors and authorized recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the contractor first receives CHRI under the approved outsourcing agreement. Enclosed is a copy of the most recent version of the Outsourcing Standard, dated November 6, 2014.

Access to the FBI-maintained CHRI is subject to numerous restrictive laws and regulations. Dissemination of such information to a private entity is prohibited except as specifically authorized by federal law or regulation. Further, the exchange of CHRI is subject to cancellation if such unauthorized dissemination is made.

Should you have any questions regarding your responsibilities in relation to the outsourcing of noncriminal justice administrative functions, please do not hesitate to contact [**insert name of CJIS Division POC**] at [**insert telephone number**], or via e-mail at [**insert e-mail address**] or me at [**insert telephone number**], or via e-mail at [**insert e-mail address**].

Respectfully,

[**Insert FBI Compact Officer's name**]  
FBI Compact Officer

Enclosure

Note: Send a copy of the response to the Compact Council Chairman and Contractor.

***Sample Language between the Authorized Recipient and Contractor regarding  
Noncriminal Justice Outsourcing Functions for Non-Channeling***

CONTRACT BETWEEN  
[AUTHORIZED RECIPIENT'S  
NAME] AND  
[CONTRACTOR'S  
NAME] REGARDING  
OUTSOURCING  
NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS

This contract is entered into between **[insert Authorized Recipient's name and address]**, the Authorized Recipient, and **[insert Contractor's name and address]**, the Contractor, under the terms of which the Authorized Recipient is outsourcing the performance of noncriminal justice administrative functions involving the handling of criminal history record information (CHRI) pursuant to Title 28, Code of Federal Regulations, Part 906 and the Security and Management Control Outsourcing Standard (Outsourcing Standard) for Non-Channelers. The most current version of the Outsourcing Standard is incorporated by reference into this contract and appended hereto as Attachment "**[insert]**".

The Authorized Recipient's authority to submit fingerprints for noncriminal justice purposes and obtain the results of the fingerprint search, which may contain CHRI, is **[insert the legal citation of the federal statutory authority or executive order that requires or authorizes the Authorized Recipient to have access to CHRI]**. This authority requires or authorizes fingerprint-based background checks of **[insert all categories of current and prospective employees, licensees, or applicants for other benefits covered by federal statutory authority or executive order]**.

The specific noncriminal justice administrative function to be performed by the Contractor that involve access to CHRI on behalf of the Authorized Recipient is to **[insert specific noncriminal justice administrative functions to be performed; i.e., missing dispositions, fitness determinations, storing criminal history record check results]**.

**[Insert Contractor's name]** will comply with the Outsourcing Standard requirements, to include the *CJIS Security Policy*, and other legal authorities to ensure adequate privacy and security of personally identifiable information and criminal history record check results related to this contract, and will ensure that all such data is returned to the Authorized Recipient as soon as no longer needed for the performance of contractual duties.

NOTE: A copy of the signature page with dates should be included with the contract.

## Outsourcing Audit Guidelines

---

If ARs are authorized to conduct national fingerprint-based background checks based on a federal statute, the FBI Compact Officer may not grant permission to outsource noncriminal justice administrative functions unless he/she has implemented a combined federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and ARs engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under an approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

Additionally, sections 2.05 of the Outsourcing Standards require certification that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement. It should be noted that each of the Outsourcing Standards places the auditing responsibility on specific parties. Specifically, the FBI will, and the AR may, conduct an audit of the Contractor performing channeling functions and the FBI is required to certify to the FBI Compact Officer that an audit was conducted. The AR will certify to the FBI Compact Officer that an audit was conducted of the Contractor performing Non-Channeling functions.

### **Sample Audit Methodology**

The purpose of the audit is to assess compliance with applicable laws, policies, regulations, and rules which pertain to access to CHRI. The audit should be scoped to cover the following areas:

- adherence to Outsourcing Standard requirements;
- use of CHRI
- dissemination of CHRI
- physical and technical security of CHRI
- compliance with other applicable laws, policies, regulations, and rules.

Agencies are encouraged to use the following sample methodology as a guide when creating the audit process. In addition, Table 2-1 graphically displays the FBI CJIS Division's outsourcing audit methodology. For additional information relating to noncriminal justice agency audits, please refer to the Council's publication *National Criminal History Record Information Audit Guide for Noncriminal Justice Agency Audits*.

#### **Pre-audit**

Appropriate representatives from ARs and Contractors selected for audit are identified and notified to discuss an overview of the audit process and scheduling of audit activities. Requests for documentation such as copies of signed contracts occur during this phase. Additionally, points-of-contact are informed that pre-audit materials will be forwarded for review and completion. Pre-audit materials are useful for gathering pertinent information prior to on-site visits and may include high-level questionnaires that are used to formulate specific questions

about agency processes, as well as data quality surveys comprised of a sampling of transactions or records that are used to validate agency processes.

### **On-Site Audit**

Administrative interviews are conducted on-site with appropriate representatives from selected ARs and Contractors. Questions focus on capturing the specific processes used by agencies to meet Outsourcing Standard requirements. In addition, on-site validation of data quality surveys is conducted. Upon completion of the on-site visit, auditors make an initial determination of compliance and conduct an exit briefing with agency personnel. On-site audit activities also include the identification of any follow-up action items necessary to complete assessments.

### **Report**

A draft audit report of findings and recommendations are completed and forwarded to AR and Contractor personnel responsible for oversight and compliance. Findings and recommendations are sufficiently detailed and directly correlate to specific policy requirements. The draft report solicits a response describing corrective actions and offering any additional comments. Upon receipt of the response, the audit report is finalized.

### **Sanctions**

Final audit reports, which incorporate comments from ARs and contractors, are forwarded to the appropriate sanctioning body for review. Upon review, the sanctioning body may consider requiring additional corrective actions or information. In addition, the sanctions process incorporates measures to elevate sanctions in a manner such that deficiencies are corrected and the risk of subsequent violations is adequately mitigated.

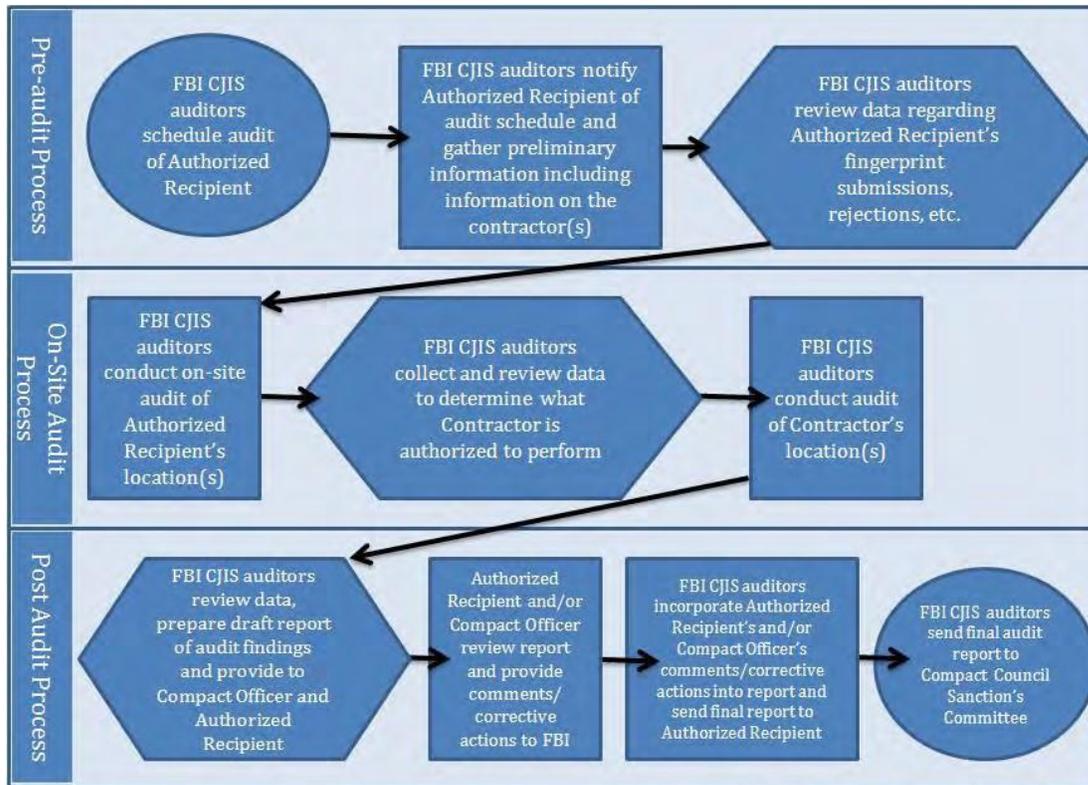


Table 2-1: Outsourcing Audit Methodology

### Sample 90 day Audit Checklist for an Authorized Recipient

The Outsourcing Standard for Non-Channelers requires ARs who have been approved to outsource noncriminal justice administrative functions conduct an audit of the Contractor within 90 days of the date that the Contractor first receives CHRI under the approved outsourcing agreement. The following chart has been designed as a tool to assist ARs who are developing an audit process to comply with the 90 day audit requirement based on the Outsourcing Standard for Non-Channelers.

The chart outlines assessment items which have been grouped topically. References to the specific requirements in the Outsourcing Standard for Non-Channelers and the *CJIS Security Policy* have also been provided for each assessment item. Depending on the function outsourced and the specifics of the process, all of the requirements listed may not be applicable.

The chart outlines assessment items which have been grouped topically. References to the specific requirements in the Outsourcing Standard for Non-Channelers and the *CJIS Security Policy* have also been provided for each assessment item. Depending on the function outsourced and the specifics of the process, all of the requirements listed may not be applicable.

### Sample 90 day Audit Checklist for an Authorized Recipient

Contractor Assessment	Reference	Yes	No	N/A
	OS-Outsourcing Standard for Non-Channelers CSP-CJIS Security Policy			
<b>Policy References</b>				
a. Copy of current Outsourcing Standard for Non-Channelers	OS 2.02, 2.03, 2.05, 2.07, 3.02, 3.03, 5.03, 6.02, 7.01, 8.01a, 9.01, 9.04, 11.05, 11.06			
b. Copy of current <i>CJIS Security Policy</i>	OS 2.03b, 2.03c, 3.01, 3.02, 3.03, 7.01, 7.02, 9.02			
<b>Security Program</b>				
a. Authorized Recipient (AR) approved minimum requirements for content of Security Program	OS 3.02			
b. Implementation of security requirements	OS 3.02, 3.03 a-d			
c. Reporting procedures for security violations	OS 3.03(c), 8.0			
<b>Security Training Program</b>				
a. AR approved	OS 3.04			
b. Training prior to appointment or assignment	OS 3.04			
c. Training upon receipt of changes	OS 3.04			
d. Annual refresher training	OS 3.04			
<b>Site Security</b>				
a. Available for announced/unannounced audits	OS 3.05			
b. Physically secure location	OS 4.01, 7.02a			
<b>Use and Maintenance of CHRI</b>				
a. Maintained in accordance with contract and does not exceed period of time AR is authorized to maintain	OS 3.07			
b. Used only in accordance with contract and AR's authority	OS 2.03, 3.01			
<b>Dissemination</b>				
a. AR approved in accordance with contract and AR's authority	OS 5.01			
b. Compliant with laws, rules, and regulations[1]	OS 5.01			
c. Log captured required information and retained for a minimum of 365 days	OS 3.08, 5.02			

<b>Personnel Security</b>				
a. Criminal background checks on all Contractor and approved sub-Contractor personnel with access to CHRI conducted prior to access	OS 6.01			
b. Confirmation of understanding by employee(s)	OS 6.02			
c. List of personnel with access to CHRI	OS 6.03			
d. Updates to list of personnel changes within 24 hours of changes	OS 6.03			

Based on OS for Non-Channelers dated 11/06/14 and CJIS Security Policy 5.3 dated 8/4/14

Page 1

[1] Applicable laws, rules, and regulations regarding the dissemination of national CHRI include Title 28, United States Code, Section 534; Title 28, Code of Federal Regulations, Section 50.12 (b) and Part 906.

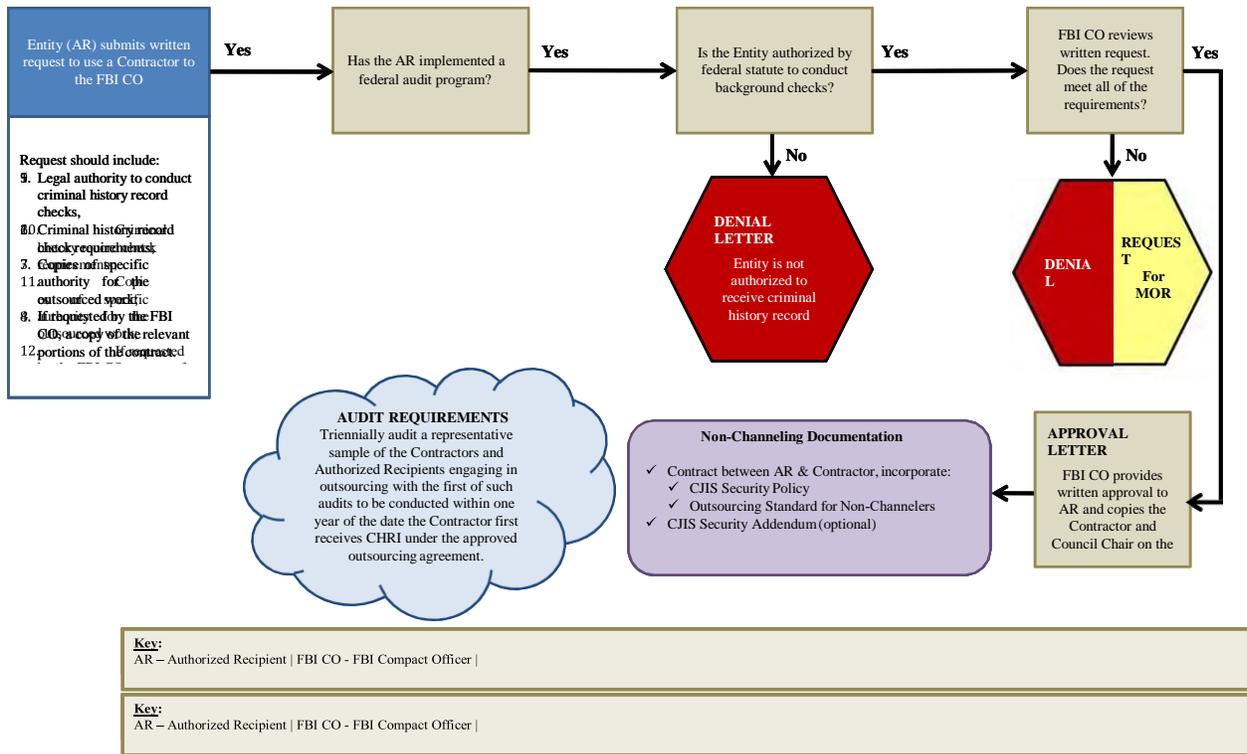
<b>Contractor Assessment</b>	<b>Reference</b>	<b>Yes</b>	<b>No</b>	<b>N/A</b>
	OS-Outsourcing Standard for Non-Channelers CSP-CJIS Security Policy			
<b>Security Violations</b>				
a. Develop and maintain written security violation plan	OS 8.01a, 2.07, 3.03			
b. Policy for disciplinary action	OS 8.01a			
c. Immediate suspension pending investigation	OS 8.01b			
d. Immediate report	OS 8.01c			
d. Follow-up report	OS 8.01c			
<b>Security on Systems Processing CHRI</b>				
a. Current topological drawing	OS 2.04			
b. Firewalls	OS 7.01a, CSP 5.10			
c. Encryption	OS 7.01b, CSP 5.5.2.4, 5.10.1.2			
f. Virus protection on networks processing CHRI	CSP 5.10.4.2			
g. User identification	CSP 5.6			
h. Authentication of user identification	CSP 5.6			
i. Advanced authentication when accessing via the Internet	CSP 5.6			
j. Audit trails	CSP 5.4.6			
<b>Media Destruction</b>				
a. Hard copy	OS 7.02c, CSP 5.8.4			
b. Electronic media	OS 7.02, CSP 5.8.3			

Based on OS for Non-Channelers dated 11/6/14 and CJIS Security Policy 5.3 dated 8/4/14

Page 2 of 2

# Non-Channeling Flowchart

Non-Channeling Flowchart



# Non- Channeling Checklist

---

## Non-Channeling Checklist

---

- Must have implemented a federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and ARs engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement.
  
- Submit the incoming request letter to include copies of the specific authority for the outsourced work, the federal requirement for the criminal history record check, and/or, if requested, a copy of relevant portions of the contract. The legal authority should be referenced in the written request.
  
- Ensure that the most current versions of both the Outsourcing Standard for Non-Channelers ([www.fbi.gov/about-us/cjis/cc/](http://www.fbi.gov/about-us/cjis/cc/)) and the *CJIS Security Policy* ([www.fbi.gov/about-us/cjis/cjis-security-policy/cjis-security-policy/view](http://www.fbi.gov/about-us/cjis/cjis-security-policy/cjis-security-policy/view)) are incorporated by reference and appended to the contract at the time of the contract and/or option renewal.
  
- Contract specifies the terms and conditions of CHRI access as specified in the Outsourcing Standard for Non-Channelers and the *CJIS Security Policy*:
  - Limit the use of such information to the purposes for which it is provided
  - Limit the retention of the information
  - Prohibit the dissemination of the information except as specifically authorized by federal laws, regulations and standards as well as rules, procedures and standards established by the Compact Council and the U.S. AG.
  - Ensure the security and confidentiality of the information to include confirmation that the Contractor is authorized to receive CHRI.
  - Provide audits and sanctions
  - Provide conditions for termination of the contract
  - Maintain up-to-date records of contractor personnel that have access to CHRI
  - Ensure contractor personnel comply with the Outsourcing Standard for Non-Channelers and the *CJIS Security Policy*
  
- Visit the Contractor's facilities for announced and unannounced audits and security inspections.
  
- Review and approve the Contractor's Security Program.
  
- Certify that an audit of the Contractor was conducted within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

## **Recommended Online Reference Materials**

---

- Security and Management Control Outsourcing Standard for Non-Channelers (current version)–  
[www.fbi.gov/about-us/cjis/cc/](http://www.fbi.gov/about-us/cjis/cc/)
- FBI *Criminal Justice Information Systems (CJIS) Security Policy* (current version) –  
[www.fbi.gov/about-us/cjis/cjis-security-policy/cjis-security-policy/view](http://www.fbi.gov/about-us/cjis/cjis-security-policy/cjis-security-policy/view)
- FBI Biometric Center of Excellence –  
[www.fbibiospecs.org](http://www.fbibiospecs.org)
- Electronic Biometric Transmission Specification (EBTS) –  
[www.fbibiospecs.org/ebts.html](http://www.fbibiospecs.org/ebts.html)

## Appendix C

### Privacy Act Statement

*This privacy act statement is located on the back of the [FD-258 fingerprint card](#).*

**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.

As of 03/30/2018

Please ensure the TGRA is using the most update to date Noncriminal Justice Applicant's Rights Notice. To view the recent notice please visit <https://www.fbi.gov/services/cjis/compact-council/guiding-principles-noncriminal-justice-applicants-privacy-rights>

#### NONCRIMINAL JUSTICE APPLICANT'S PRIVACY RIGHTS

As an applicant who is the subject of a national fingerprint-based criminal history record check for a noncriminal justice purpose (such as an application for employment or a license, an immigration or naturalization matter, security clearance, or adoption), you have certain rights which are discussed below. All notices must be provided to you in writing.<sup>1</sup> These obligations are pursuant to the Privacy Act of 1974, Title 5, United States Code (U.S.C.) Section 552a, and Title 28 Code of Federal Regulations (CFR), 50.12, among other authorities.

- You must be provided an adequate written FBI Privacy Act Statement (dated 2013 or later) when you submit your fingerprints and associated personal information. This Privacy Act Statement must explain the authority for collecting your fingerprints and associated information and whether your fingerprints and associated information will be searched, shared, or retained.<sup>2</sup>
- You must be advised in writing of the procedures for obtaining a change, correction, or update of your FBI criminal history record as set forth at 28 CFR 16.34.
- You must be provided the opportunity to complete or challenge the accuracy of the information in your FBI criminal history record (if you have such a record).
- If you have a criminal history record, you should be afforded a reasonable amount of time to correct or complete the record (or decline to do so) before the officials deny you the employment, license, or other benefit based on information in the FBI criminal history record.
- If agency policy permits, the officials may provide you with a copy of your FBI criminal history record for review and possible challenge. If agency policy does not permit it to provide you a copy of the record, you may obtain a copy of the record by submitting fingerprints and a fee to the FBI. Information regarding this process may be obtained at <https://www.fbi.gov/services/cjis/identitv-history-summary-checks> and <https://www.edo.cjis.gov>.
- If you decide to challenge the accuracy or completeness of your FBI criminal history record, you should send your challenge to the agency that contributed the questioned information to the FBI. Alternatively, you may send your challenge directly to the FBI by submitting a request via <https://www.edo.cjis.gov>. The FBI will then forward your challenge to the agency that contributed the questioned information and request the agency to verify or correct the challenged entry. Upon receipt of an official communication from that agency, the FBI will make any necessary changes/corrections to your record in accordance with the information supplied by that agency. (See 28 CFR 16.30 through 16.34.)
- You have the right to expect that officials receiving the results of the criminal history record check will use it only for authorized purposes and will not retain or disseminate it in violation of federal statute, regulation or executive order, or rule, procedure or standard established by the National Crime Prevention and Privacy Compact Council.<sup>3</sup>

<sup>1</sup> Written notification includes electronic notification, but excludes oral notification.

<sup>2</sup> <https://www.fbi.gov/services/cjis/compact-council/privacy-act-statement>

<sup>3</sup> See 5 U.S.C. 552a(b); 28 U.S.C. 534(b); 34 U.S.C. § 40316 (formerly cited as 42 U.S.C. § 14616), Article IV(c); 28 CFR 20.21(c), 20.33(d) and 906.2(d).

Updated 11/6/2019

## Appendix D

### NIGC Fingerprint System Security, Protocols and Data Requirements

#### System Security

Communication between the Tribe and the NIGC Fingerprint Internet System occurs through the exchange of Internet mail messages over a secure network connection. As mentioned, the Tribe will submit EFTS compliant submissions and receive FBI results using email through a Virtual Private Network (VPN). Agencies will be required to authenticate themselves using strong mechanisms and robust protocols and algorithms to protect the confidentiality and integrity of information being transmitted over the Internet.

The communications system the Tribe will use is the NIGC Internet Security Services (ISS). The ISS provides Group Authentication to the Tribe which is needed to support these enhanced functions. When contacted by the Tribe, the NIGC Fingerprint Administrator will provide to the Tribe the Group Authentication username and password.

*The enhanced VPN supported is an end to end SSL Point to Point encryption based on NIST 104-2.*

#### System Protocol(s):

The NIGC's Fingerprint Internet Mail server and the NIGC's AltaScan SnF requires that submitting system(s) send fingerprint submissions using the Simple Mail Transfer Protocol (SMTP). SMTP is a TCP/IP application that allows the transfer of mail from one system to another. The details of this protocol are defined by the following standards:

- 1) RFC 821 – Simple Mail Transfer Protocol (SMTP)
- 2) RFC 822 – Standard for the format of ARPA Internet text messages
- 3) RFC 1652 – SMTP Service extensions for 8-bit MIME transport
- 4) RFC 1521 – MIME Part One: Mechanisms for specifying and describing the format of Internet Message Bodies
- 5) RFC 1522 – MIME Part Two: Message header extensions for NON-ASCII Text

NOTE: The SMTP system must be compatible with the above RFC's.

The body of the SMTP message must be base-64, MIME encoded and single part. The header of the message should include the following parameters:

**Date:**  
**From:**  
**To:**  
**Subject:**  
**MIME-Version:**  
**Content-type:**

## **Content-Transfer-Encoding:**

The field contents are defined as:

**Date:** The date and time of which the SMTP message was sent.

**From:** The mail address, in the form of user@host.domain from which the message was sent. This address will be specified by the NIGC. This will also define the address of the POP3 mailbox to which the NIGC SnF sends the SRE (NIST) responses. This is provided on the Pre-Activation Checklist.

**To:** The mail address, in the form of user@host.domain, defines where the message will be sent. This is provided on the Pre-Activation Checklist.

**Subject:** This field contains the message subject. This field should always be set to “Electronic Ten Print Submissions”

**MIME-Version:** This field specifies the MIME version used to encode the data.

**Content-Type:** This field specifies the type of body contained in the mail message (application/octet-stream) and an additional attribute for the attachment name (name=efts.sub). The attachment name should be separated by a semi-colon and should always be efts.sub for all 10 print submissions to the NIGC SnF.

**Content-Transfer-Encoding:** This field specifies the encoding algorithm that was used on the body of the message. This field should always be set to base 64.

When sending a compliant SMTP message, the *typical* SMTP header will look like the following example:

```
Date: Wed May 10 14:25:16 2000
From: tribe@nigcext01.nigc.gov
To: triberelay@nigcext01.nigc.gov
Subject: AltaScan Electronic Ten Print Submissions
MIME-Version: 1.0
Content-type: application/octet-stream; name=efts.sub
Content-Transfer-Encoding: base64
```

## **Data Requirements:**

All Electronic ten-print submissions to the NIGC SnF must be compliant with the ANSI NIST/EFTS 6.2 or EFTS 7.0 standards. The minimum record set includes type 1, 2 and 4 records for each submission. All EFTS mandatory fields must be sent on the submission, (See Tables 1 and 2 for a complete list of descriptors). In addition, the following EFTS fields should contain the provided data elements to meet the NIGC’s requirements:

- 1.04 – TOT The Type of Transaction must be “FAUF” or Federal Applicant User Fee.
- 1.07 – DAI The Designation Agency Identifier (DAI) should contain the value “WVIAFIS0Z”.  
**NOTE:** There is a zero (0) before the Z.
- 1.08 – ORI The Originating Agency Identifier (ORI) should contain “USNIGC00Z”. **NOTE:** There are two zeros (0) before the Z.
- 1.09 – TCN The Transaction Control Number (TCN) must be at least 10 characters and no more than 40 in length with the first 6 characters being the first 6 letters of your Originating Agency Case (OCA) code. **NOTE:** The SnF does not allow any duplicate TCN regardless if the duplicate is from two separate Agencies. If more than one submission with the same TCN is received by the SnF, the second and subsequent submissions will be rejected.
- 1.10 – TCR The Transmission Control Reference (TCR) should contain the IAFIS TCR number if sending a no-charge resubmission. The TCR number is obtained from your IAFIS response. This is the E200... number. The FBI will allow one free resubmission for an applicant. If the resubmission returns an error, the FBI will process the third resubmission as a new submission and bill you. **NOTE:** Leave this field blank if not sending a no-charge resubmission.
- 2.009 – OCA The Originating Agency Case Number must contain the OCA number assigned by the NIGC.
- 2.016 – SSN The applicant’s Social Security Number. **NOTE:** This field is required for the NIGC.
- 2.037 – RFP The Reason Fingerprinted. **NOTE:** This field should contain “Indian Gaming Licensee”
- 2.073 – CRI The Contributor Agency Identifier (CRI) field must also contain “USNIGC00Z”.  
**NOTE:** There are two zeros (0) before the Z.

## Table 1. EFTS/NIGC Descriptors

### Type 1 NIST Data Descriptors

Identifier	Field Number	Field Name	Character Type	Field Size Per Occurrence		Occurrences		O/M Opt. / Mand.
				Min	Max	Min	Max	
LEN	1.01	Logical Record Length	N	2	3	1	1	M
VER	1.02	Version Number	N	4	4	1	1	M
CNT	1.03	File Content	N	9	48	1	1	M
TOT	1.04	Type Of Transaction	A	4	4	1	1	M
DAT	1.05	Date	N	8	8	1	1	M
PRY	1.06	Priority	N	1	1	0	1	M Default to 2.
DAI	1.07	Destination Agency Identifier	AN	9	9	1	1	M
ORI	1.08	Originating Agency Identifier	AN	9	9	1	1	M
TCN	1.09	Transaction Control Number	ANS	10	40	1	1	M
TCR	1.10	Transaction Control Reference	ANS	10	40	0	1	O
NSR	1.11	Native Scanning Resolution	NS	5	5	1	1	M
NTR	1.12	Nominal Transmitting Resolution	NS	5	5	1	1	M

Items in blue have special NIGC requirements beyond those of the EFTS. (See Section above - Data Requirements)

## Table 2. EFTS/NIGC Descriptors Continued

### Type 2 NIST Data Descriptors

Data Elements	NIST Field Number	Field Type Alpha Numeric Special	Field Size		Occurrences		O/M Optional/ Mandatory
			Min	Max	Min	Max	
Logical Record Length	2.001	N	2	7	1	1	M
Image Designation Character	2.002	N	2	2	1	1	M
Retention Code	2.005	A	1	1	1	1	M
Attention Indicator	2.006	ANS	3	30	0	1	O
Send Copy To	2.007	ANS	9	19	0	9	O
Originating Agency Case Number	2.009	ANS	9	9	1	1	M
FBI Number	2.014	AN	1	9	0	5	O
Social Security Number	2.016	N	9	9	0	4	M
Miscellaneous Identification Number	2.017	ANS	4	15	0	4	O
Name	2.018	AS	3	30	1	1	M
Aliases	2.019	ANS	3	30	0	10	O
Place of Birth	2.020	A	2	2	1	1	M
Country of Citizenship	2.021	A	2	2	0	1	O
Date of Birth	2.022	N	8	8	1	5	M
Sex	2.024	A	1	1	1	1	M
Race	2.025	A	1	1	1	1	M
Scars, Marks, Tattoos	2.026	AS	3	10	0	10	O
Height	2.027	AN	3	3	1	1	M
Weight	2.029	N	3	3	1	1	M
Eye Color	2.031	A	3	3	1	1	M
Hair Color	2.032	A	3	3	1	1	M
Reason Fingerprinted	2.037	ANS	1	75	1	1	M
Date Printed	2.038	N	8	8	1	1	M
Employer and Address	2.039	ANS	1	120	0	1	O
Occupation	2.040	ANS	1	50	0	1	O
Residence of Person Fingerprinted	2.041	ANS	1	120	0	1	O
Military Code	2.042	A	1	1	0	1	O
Image Capture Equipment	2.067	ANS			0	1	O
Make			1	25	1	1	M
Model			1	25	1	1	M
Serial No.			1	50	1	1	M
Request for Rap Sheet	2.070	A	1	1	0	1	O
Controlling Agency Identifier	2.073	ANS	9	9	1	3	M
Amputated or Bandaged	2.084	C			0	9	Condit.
Finger Number		N	2	2	1	1	M
Amp/Ban Code		A	2	2	1	1	M

# Appendix E

## CJIS Name Check Request

Please Type or Print Clearly

Please complete the attached form to request a name check. Please be advised that an individual's fingerprints must be rejected twice for technical issues prior to requesting a name check.

\*ORI of State/Federal/Regulatory Agency: USNIGC00Z

\*Your agency's Point of Contact (POC) for the response: Seneca Chavis

\*Phone number of POC: 202-632-0298

\*Fax number of POC: 202-606-4935

\*Name and Address of requesting agency:

NIGC

90 K Street, N.E., Ste. 200

Washington, DC 20002

C/O Department of the Interior 1849

C Street N.W.

Mail Stop #1621 Washington,

D.C., 20240

Response will be faxed.

\*Please complete all the below fields.

---

### Subject of Name Check

Two Transaction Control Numbers (TCN, E#'s) of the subjects fingerprint submission:

(1) E2020

(2) E2020

\*Name: \_\_\_\_\_ \*Alias: \_\_\_\_\_

\*Date of Birth: \_\_\_\_\_ Place of Birth: \_\_\_\_\_ Sex: \_\_\_\_\_ Race: \_\_\_\_\_

\*Social Security Number: \_\_\_\_\_ Miscellaneous Number: \_\_\_\_\_

State Identification Number: \_\_\_\_\_ OCA: \_\_\_\_\_

Please note the asterisked fields are required for Name Check searches, all other fields are optional. Results provided will be the results of biographical information included in the original fingerprint submission.

## Appendix F

### Example Noncriminal Justice Agency Policies and Procedures

Revised June 20, 2018

Note: Please read these policies in their entirety. You cannot simply copy and paste your Tribe name on these policies for them to be complete or accurate. You must also customize these policies to reflect your Tribe-specific procedures. Everything listed here will be verified during the audit process.

As a guideline, text that is highlighted in yellow is where you enter your Tribe name.

Text that is highlighted in green is either instructions for you or a decision that you must make to reflect your policies. Remove/modify the applicable text from the final document as needed.

#### GENERAL ADMINISTRATION

##### I. Purpose

**Tribe Name** may use the Criminal Justice Information (CJI) or Criminal History Record information (CHRI) obtained from the Arizona Department of Public Safety (DPS) only for the specific purpose of evaluating **(state the purpose from your user agreement - i.e. employees, volunteers, contractors, licenses, etc.)**. CJI/CHRI may not be reused for any other purpose.

##### II. Authority

**Tribe Name** has the authorization to submit fingerprints to the National Indian Gaming Commission for Federal Criminal History Checks pursuant to **(list your authority here (i.e. specific Arizona state law, executive order, local ordinance, tribal resolution, etc.))**. The authority is listed in the Noncriminal Justice User Agreement between the National Indian Gaming Commission and **Tribe Name**.

##### III. Local Agency Security Officer (Primary Liaison)

**Tribe Name's Local** Agency Security Officer (LASO) is the point of contact with the NIGC through which all communication with the NIGC regarding audits, Tribe/personnel information changes and training and security are conducted. The LASO will maintain all authorized personnel training on the NCJA Training Documentation Form (or similar document). This information will be available at time of audit. The LASO can receive and disseminate communication updates from the NIGC. For the responsibilities of the LASO, refer to the Local Agency Security Officer Basic Responsibility worksheet in the training handouts.

##### IV. Authorized Personnel

**Tribe Name's** Gaming Commission (GC) staff may encounter CJI/CHRI. Authorized personnel will be given access to view and handle the CJI/CHRI after completing the required training (CJIS Online Security & Awareness training and reading our Tribe- specific policies and procedures) and the one-time signing of an acknowledgement statement. The Authorized Personnel consists of **(list specific job titles or departments here as needed)**, and designated Local Agency Security Officer (LASO). Refer to the Authorized Personnel List for the most current authorized personnel. The authorized personnel are aware of the other personnel on this list. Upon termination of authorized personnel, the LASO will update the Authorized Personnel List with the NIGC as soon as possible.

The personnel listed on the current Authorized Personnel List on file with the NIGC **Access Integrity Unity (AIU)** are the only personnel authorized to access, discuss, use, handle, disseminate, file, log and destroy the CJI/CHRI. To prevent tampering, all terminated personnel, the public, all outside persons and entities are prohibited from handling or having any access to CJI/CHRI for any reason. Secondary dissemination to an outside agency is prohibited.

**If your Tribe does not store CJI/CHRI electronically then remove this entire highlighted paragraph. Only authorized personnel have access to the electronic secured and encrypted database where brief information of the CJI/CHRI are electronically stored. To prevent tampering or unauthorized access, once the authorized personnel is done entering or reviewing information, they must lock the database and log off the computer. Refer to the Storage of CJI/CHRI section below for more information regarding electronic storage. Remove the previous sentence if you do not list more information in the Storage of CJI/CHRI section.**

**Tribe Name** does not store CJI/CHRI electronically.

To prevent unauthorized access or tampering, the fingerprint filing cabinet and drawers are locked throughout the day and one key is secured with the LASO and one other key is secured with the designated authorized personnel. All visitors to the area where CJI/CHRI are kept are accompanied by authorized staff personnel as well.

The Non-Criminal Justice Applicant Fingerprint Card Inventory Sheet(s) must be retained for auditing purposes. The National Indian Gaming Commission is on a three-year auditing cycle and can request to see the previous year's inventory sheets. For example, if the audit is being conducted in 2018, the inventory sheets from 2017 must be made available if requested.

Where possible, have personnel on the Authorized Personnel List been fingerprinted? As there is no Arizona state law existing as a specific authorization, this is not currently required. State if you are able to do this however. For example, many agencies in this program have a user agreement that states the purpose is for employment. In this example you could fingerprint the personnel on your list. If your purpose is adoption certification, then obviously you could not fingerprint the personnel on your list. Personnel with a felony conviction should not have access to CJI/CHRI.

## FINGERPRINT SUBMISSIONS

## v. Fingerprint Card Processing

**Tribe Name** requires that all applicants must provide a valid, unexpired form of government-issued photo identification during the application process and prior to fingerprinting to verify their identity. Accepted forms of primary and secondary identification have been approved through the National Crime Prevention and Privacy Compact Council Identity Verification Program Guide.

A copy of the applicant's FBI Privacy Rights Notification will be provided to the applicant prior to fingerprinting.

**Tribe Name** requires that all applicants must be fingerprinted if they are **(state the purpose from your user agreement - i.e. employees, volunteers, contractors, licenses, etc.)**. Applicants that have disclosed a conviction will be fingerprinted as well. **Applicants are fingerprinted on-site at the Tribe Name's Gaming Commission office or the fingerprint card is given/mailed to the applicant to take to their local police department to get fingerprinted.**

If you mail fingerprint cards to applicants you need to include a chain of custody form so that the fingerprinter can verify the applicant's identity at the time of fingerprinting. A sample form can be found in the NCJ Agency Guide Appendix A. The fingerprinter should be sealing the envelope the fingerprints are mailed in so that the applicant cannot tamper with them. State here if you are doing this and how.

**Tribe's Name** designated Gaming Commission staff takes possession of the fingerprint card and will ensure the correct purpose and authority (see above) are written on the fingerprint card in the "reason fingerprinted" box. Once the fingerprint card is completed and at no point in time is the fingerprint card to be returned to the applicant. Chain of custody procedures are maintained to protect the integrity of the applicant's fingerprints prior to submission to the NIGC and/or the FBI.

The fingerprint cards are then placed in a manila folder and then into a locked drawer to be mailed with the inventory sheet to the NIGC. Only authorized personnel have access to this locked drawer and the key is stored in the LASO's office.

When a fingerprint card is mailed or provided to the applicant, authorized personnel or designated Gaming Commission staff will provide a packet that contains the following:

- Pre-filled fingerprint card with the employer's address, reason for fingerprint (authorization and purpose) and OCA number.
- A sealable envelope pre-labeled with the employer's address and a space marked with an X on the back of this envelope for the fingerprint technician to sign on the line provided.
- Applicant FBI Privacy Rights Notification.
- Instructions for the applicant on how to handle and return the fingerprint card in the provided envelope.
- Fingerprint technician instructions.

If the envelope shows evidence of opening or tampering, the applicant will be asked to provide another fingerprint card and authorized personnel will repeat the procedures to issue a new fingerprint card.

If your Tribe performs its own fingerprinting then delete this paragraph. If your Tribe sends applicants off-site to be fingerprinted, ensure you state here what your procedures are for ensuring the fingerprinter is verifying the identity of the applicant and how the fingerprints are being safeguarded until they are returned to your Tribe prior to submission to DPS. Does the fingerprinter mail the fingerprints to your Tribe or do they give them back to the applicant?

## PRIVACY & SECURITY

### VI. Handling/Retention of CJI/CHRI

The fingerprint results from the NIGC are delivered in a sealed envelope clearly labelled “National Indian Gaming Commission”. This mail should be considered to contain CJI/CHRI and should only be provided directly to authorized personnel or the LASO. Only authorized personnel will open mail that contains the CJI/CHRI.

During the course of suitability determination, here are the steps that authorized personnel will follow:

- **If your Tribe does not store CJI/CHRI electronically then remove this bullet point. A summary of the CJI/CHRI are stored electronically on the Gaming Commission secured and encrypted drive with only authorized personnel having access.**
- Before suitability is determined, the CJI/CHRI is stored in a locked drawer for the authorized personnel to review and make a suitability determination.
- After suitability is determined, the CJI/CHRI is stored in a separate employee fingerprinting file. These records cannot be released for any public records request.
- After the final determination is rendered, the CJI/CHRI are filed in the fingerprint filing cabinet which is locked throughout the day and all visitors to the area are accompanied by designated Gaming Commission staff or authorized personnel.

State here if your Tribe retains CJI/CHRI and for how long. If you are not retaining CJI/CHRI state that it is destroyed after a hiring decision or after any appeals process has been completed.

### VII. Communication

Authorized Personnel may discuss the contents of the CJI/CHRI with the applicant in a private secure place and extreme care should be taken to prevent overhearing, eavesdropping or interception of communication. The applicant may not be given a copy of the record or allowed to take a picture of it with an electronic device. The record is for **Tribe Name's** use only.

Employees will not confirm the existence or non-existence of an individual's criminal history record to the public or to any unauthorized individual. The applicant should be informed that if he/she wishes to challenge the content of the record, they can contact:

- For a copy of an FBI criminal history record contact the FBI at 304-625-5590. More information can be found at <https://www.fbi.gov/services/cjis/identity-history-summary-checks>

**Tribe Name** provides all applicants the right to review and challenge his/her criminal history record if they deem the information has been inaccurately reported. Each applicant will be provided **(let applicants know how many days you are providing them to challenge their record)** upon notification to provide **Tribe Name** authentic documentation that reports the criminal history information accurately and completely. This information must be provided prior to determination of suitability for **(state the purpose from your user agreement - i.e. employees, volunteers, contractors, licenses, etc.)**.

CJI/CHRI shall not be copied, emailed, faxed or scanned nor disseminated to secondary parties or the employee. Any casual unauthorized release of information is not allowed (i.e. social media, discussion with friends or family members). CJI/CHRI shall only be discussed (written or verbally) between the authorized personnel as necessary to carry out the specific purpose for which the information was requested and all verbal discussions take place in private.

If the fingerprint-based check has a disqualifying factor, the authorized personnel who opened and reviewed the record will hand-carry the record to the ASC or occasionally other authorized personnel, to determine the next steps. The ASC or authorized personnel will discuss the contents of the record with the applicant in a private and secure manner to obtain any additional information.

**If your Tribe does not have an appeals process for an initial denial of employment, etc. then remove this paragraph.** **Tribe Name** will provide applicants with an appeals process. The appeals process can take place when the applicant challenges his/her suitability determination made by those on the authorized personnel list. This process concludes with the **(title of individual)** making the final suitability determination.

#### VIII. Storage of CJI/CHRI

Once the CJI/CHRI has met its purpose, it is filed by authorized personnel in a secured locked filing cabinet in the Gaming Commission office in a secure location. CJI/CHRI are retained in accordance with **Tribe Name's** record retention policy. This CJI/CHRI filing cabinet does not contain any other employment records or any files which may be considered public record to prevent unauthorized access or dissemination. The filing cabinet is locked throughout the day to prevent unauthorized access by non-authorized personnel. The keys to the filing cabinet are kept secure by the LASO and another back-up key is kept secure with other authorized personnel. Only authorized personnel are allowed access to the filing cabinets that contain the CJI/CHRI. If a key to the filing cabinet that contains the records is lost, the filing cabinet will be re-keyed to prevent unauthorized access.

Authorized personnel are responsible for safeguarding the confidentiality of the information at all times and may not disclose or allow access to the information to anyone except authorized

personnel. CJI/CHRI is always secured and never left unattended.

**If your Tribe does not store CJI/CHRI electronically then remove this paragraph.** The actual copy of the CJI/CHRI results are not electronically stored, but as mentioned above in section VI. Handling/Retention of CJI/CHRI, some essential information is entered for reference and tracking purposes and electronically stored. Physical protection of CJI/CHRI as well as a physically secure location for CJI/CHRI will be shared and verified with the DPS. The database where the CJI/CHRI is stored is in the **Tribe Name Gaming Commission server** which is secure, encrypted and controlled directly by **Tribe Name**. No other organization has access to this database. All visitors to the area where CJI/CHRI are stored electronically are accompanied by authorized personnel.

#### IX. FBI notifications

The authorized personnel will provide a copy of the FBI Applicant's Privacy Rights Notification to the applicant when they arrive to be fingerprinted. Copies of the FBI Applicant's Privacy Rights Notification are available at the front desk and it will contain the following information:

- Your fingerprints will be used to check the criminal history records of the FBI. If you have a criminal history record, the officials making a determination of your suitability for the job, license, or other benefits must provide you the opportunity to complete or challenge the accuracy of the information in the record. You should be afforded a reasonable amount of time **(your Tribe must define what reasonable means, i.e. 5 days, etc.)** to correct or complete the record (or decline to do so) before officials deny you the job, license, or other benefits based on information in the criminal history record.
- The procedures for obtaining a change, correction or updating of your FBI criminal history record are set forth in Title 28 Code of Federal Regulations, section 16.30 through 16.34. Information on how to review and challenge your FBI criminal record can be found at [www.fbi.gov](http://www.fbi.gov) under Identity History Summary Checks or by calling 304-625-5590.

#### X. Disposal of CJI/CHRI

When the CJI/CHRI has met the destruction date in accordance with **Tribe Name's** record retention policy, authorized personnel will destroy the CJI/CHRI. **State how you destroy CJI/CHRI (either shredding or burning).**

In the event of a third-party contractor that performs the shredding, authorized personnel will accompany the vendor to oversee the shredding and handling of the CJI/CHRI. The authorized personnel, will observe the contractor from the time the shredding receptacle is picked up through the complete destruction of the CJI/CHRI.

#### XI. Misuse of CJI/CHRI

In the event of deliberate, reckless or unintentional misuse of CJI/CHRI, the employee will be disciplined in accordance with the signed acknowledgement statement and **Tribe Name's**

**Gaming Commission** policy which can include termination.

**XII. Training and Acknowledgement Statements**

All authorized personnel must be trained in the online security awareness (CJIS Online) training within six months of hire (or upon being added to the Authorized Personnel List) and then every two years thereafter.

All authorized personnel must be trained in all in-house privacy and security training on the access, use, handling, dissemination and destruction procedures regarding CJI/CHRI within six months of hire (or upon being added to the Authorized Personnel List) and then every two years thereafter.

All authorized personnel will sign an acknowledgement statement regarding the notification of the penalties for misuse of CJI/CHRI.

All training and acknowledgement statements will be recorded on a training documentation log. This log is reviewed during audits by the NIGC.

## Acceptable Use Policy

### **1.0 Overview**

The intention for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to <Agency Name> established culture of openness, trust, and integrity. <Agency's Security Team> is committed to protecting <Agency Name>'s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, File Transfer Protocol, and National Crime Information Center access are the property of the <Agency Name>. These systems are to be used for business purposes in serving the interests of the agency in the course of normal operations. Effective security is a team effort involving the participation and support of every <Agency Name> employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

### **2.0 Purpose**

The purpose of this policy is to outline the acceptable use of computer equipment at <Agency Name>. These rules are in place to protect the employee and <Agency Name>. Inappropriate use exposes <Agency Name> to risk including virus attacks, compromises of the network systems and services, and legal issues.

### **3.0 Scope**

This policy applies to employees, contractors, consultants, temporary staff, and other workers at <Agency Name>, including all personnel affiliated with NCIC and third parties. This policy applies to all equipment that is owned or leased by <Agency Name>.

## **4.0 Policy**

### **4.1 General Use and Ownership**

1. While <Agency Name's> network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of the <Agency Name>. Because of the need to protect <Agency Name's> network, management cannot guarantee the confidentiality of information stored on any network device belonging to <Agency Name>.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should consult their supervisor or management.
3. <Agency Name> security department recommends that any information that a user considers sensitive or vulnerable (etc. residual NCIC information on a computer terminal that has access to the internet and CJIS information) be encrypted. For guidance on information classification, see <Agency Name> Information Classification Policy.
4. For security and network maintenance purposes, authorized individuals within <Agency Name> may monitor equipment, systems and network traffic at any time, per <Agency Name> Audit Policy>.
5. <Agency Name> reserves the right to audit the network and systems on a periodic basis to ensure compliance with this policy.

## **4.2 Security and Proprietary Information**

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or non-confidential, as defined by agency confidentiality guidelines. Examples of confidential information include, but are not limited to: NCIC information, state criminal history information, agency personnel data, etc. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Please review <Agency Name's> Password Policy for guidance.
3. All personal computers, laptops, and workstations should be secured with password-protected screen savers with an automatic activation feature, set at ten minutes or less, or by logging off (control-alt-delete) when the computer is unattended.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with "Laptop Security Policy".
5. All devices used by employees that are connected to the <Agency Name> Internet/Intranet/Extranet, whether owned by the employee or <Agency Name>, shall be continually executing approved virus-scanning software with a current database.

6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

### **4.3 Unacceptable Use**

The following activities are, in general, prohibited. Under no circumstances is an employee of <Agency Name> authorized to engage in any activity that is illegal under local, state, federal, or international law utilizing <Agency Name> owned resources. The list below are by no means exhaustive, but attempts to provide a frame work for activities which fall into the category of unacceptable use.

### **4.4 System and Network Activities**

The following activities are strictly prohibited, with no exceptions:

1. Unauthorized access, copying, or dissemination of classified or sensitive information (e.g., NCIC information, state criminal information, etc.).
2. Installation of any copyrighted software for which <Agency Name> or end user does not have an active license is strictly prohibited.
3. Installation of any software without preapproval and virus scan is strictly prohibited.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, logic bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others.
6. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For the purpose of this policy, “disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
7. Port scanning or security scanning is expressly prohibited unless prior notification has been given to <Agency Name> Security administration.
8. Executing any form of network monitoring which will intercept data not intended for the employee’s host, unless this activity is a part of the employee’s normal job/duty.
9. Circumventing user authentication or security of any host, network, or account.

10. Interfering with or denying service to any user other than the employee's host.
11. Using any program/script/command or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about NCIC or list of <Agency Name> employees to parties outside <Agency Name>.

## **5.0 Enforcement**

Violations of this policy include, but are not limited to: accessing data to which the individual has no legitimate right; enabling unauthorized individuals to access data; disclosing data in a way that violates applicable policy, procedures, or relevant regulations or law; inappropriately modifying or destroying data; inadequately protecting restricted data. Any violation of this policy may result in network removal, access revocation, corrective or disciplinary action, civil or criminal prosecution, and termination of employment.

## DISCIPLINARY POLICY

In support of *[Agency Name]*'s mission of public service to the city of/county of *[city or county name]* citizens, the *[Agency Name]* provides the needed technological resources needed to personnel to access FBI CJIS systems and information in support of the agency's mission. All agency personnel, with access to FBI Criminal Justice Information (CJI) or any system with stored FBI CJI, have a duty to protect the system and related systems from physical and environmental damage and are responsible for correct use, operation, care and maintenance of the information. All technology equipment: computers, laptops, software, copiers, printers, terminals, MDTs, mobile devices, live scan devices, fingerprint scanners, software to include RMS/CAD, operating systems, etc., used to process, store, and/or transmit FBI CJIS is a privilege allowed by *[Agency Name]*, state CSO, and the FBI. To maintain the integrity and security of the *[Agency Name]*'s and FBI's CJIS systems and data, this computer use privilege requires adherence of relevant federal, state and local laws, regulations and contractual obligations. All existing laws and *[Agency Name]* regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply to personal conduct.

Misuse of computing, networking or information resources may result in temporary or permanent restriction of computing privileges up to employment termination. In some misuse situations, account privileges will be suspended to prevent ongoing misuse while under investigation. Additionally, misuse can be prosecuted under applicable statutes. All files are subject for search. Where follow---up actions against a person or agency after an information security incident involves legal action (either civil or criminal), the evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). Complaints alleging misuse of *[Agency Name]*'s computing and network resources and FBI CJIS systems and/or data will be directed to those responsible for taking appropriate disciplinary action.

### *Examples of Misuse with access to FBI CJI*

1. Using someone else's login that you are not the owner.
2. Leaving computer logged in with your login credentials unlocked in a physically unsecure location allowing anyone to access *[Agency Name]* systems and/or FBI CJIS systems and data in your name.
3. Allowing unauthorized person to access FBI CJI at any time for any reason. Note: Unauthorized use of the FBI CJIS systems is prohibited and may be subject to criminal and/or civil penalties.
4. Allowing remote access of *[Agency Name]* issued computer equipment to FBI CJIS systems and/or data without prior authorization by *[Agency Name]*.
5. Obtaining a computer account that you are not authorized to use.
6. Obtaining a password for a computer account of another account owner.
7. Using the *[Agency Name]*'s network to gain unauthorized access to FBI CJI.
8. Knowingly performing an act which will interfere with the normal operation of FBI CJIS systems.
9. Knowingly propagating a computer virus, Trojan horse, worm and malware to circumvent data protection or compromising existing security holes to FBI CJIS systems.
10. Violating terms of software and / or operating system licensing agreements or copyright laws.
11. Duplication of licensed software, except for backup and archival purposes that circumvent copyright laws for use in *[Agency Name]*, for home use or for any customer or contractor.

12. Deliberately wasting computing resources to include streaming audio, videos for personal use that interferes with *[Agency Name]* network performance.
13. Using electronic mail or instant messaging to harass others.
14. Masking the identity of an account or machine.
15. Posting materials publicly that violate existing laws or *[Agency Name]*'s codes of conduct.
16. Attempting to monitor or tamper with another user's electronic mail or files by reading, copying, changing, or deleting without explicit agreement of the owner.
17. Using *[Agency Name]*'s technology resources to advance unwelcome solicitation of a personal or sexual relationship while on duty or through the use of official capacity.
18. Unauthorized possession of, loss of, or damage to *[Agency Name]*'s technology equipment with access to FBI CJI through unreasonable carelessness or maliciousness.
19. Maintaining FBI CJI or duplicate copies of official *[Agency Name]* files in either manual or electronic formats at his or her place of residence or in other physically non-secure locations without express permission.
20. Using *[Agency Name]*'s technology resources and/or FBI CJIS systems for personal or financial gain.
21. Deliberately failing to report promptly any known technology-related misuse by another employee that may result in criminal prosecution or discipline under this policy.
22. Using personally owned devices on *[Agency Name]*'s network to include personally-owned thumb drives, CDs, mobile devices, tablets on wifi, etc. Personally owned devices should not store *[Agency Name]* data, State data, or FBI CJI.

The above listing is not all-inclusive and any suspected technology resource or FBI CJIS system or FBI CJI misuse will be handled by *Agency Name* on a case by case basis. Activities will not be considered misuse when authorized by appropriate *Agency Name* officials for security or performance testing.

#### *Privacy Policy*

All agency personnel utilizing agency-issued technology resources funded by *[Agency Name]* expressly acknowledges and agrees that such service, whether for business or personal use, shall remove any expectation of privacy. Use of *[Agency Name]* systems indicates consent to monitoring and recording. The *[Agency Name]* reserves the right to access and audit any and all communications including electronic and physical media at rest, in transit and at end of life. *[Agency Name]* personnel shall not store personal information with an expectation of personal privacy that are under the control and management of *[Agency Name]*.

#### *Personal Use of Agency Technology*

The computers, electronic media and services provided by *[Agency Name]* are primarily for business use to assist personnel in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their business purposes. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

#### *Misuse Notification*

Due to the increase in the number of accidental or malicious computer attacks against both government and private agencies, *[Agency Name]* shall: (i) establish an operational incident handling capability for all information systems with access to FBI CJIS systems and data. This includes adequate preparation,

detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security---related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level.

All *[Agency Name]* personnel are responsible to report misuse of *[Agency Name]* technology resources to appropriate *[Agency Name]* officials.

Local contact---LASO: [firstnamelast@agencyname.com](mailto:firstname.lastname@agencyname.com) Phone:

State contact---CSA ISO: [firstnamelast@state.gov](mailto:firstname.lastname@state.gov) Phone:

I have read the policy and rules above and I will abide in the *[Agency Name]*'s Disciplinary

policy. Signature: \_\_\_\_\_ Date: \_\_\_\_\_/20\_\_\_\_\_

## Disposal of Media Policy and Procedures

### 1.0 Purpose

The purpose of this policy is to outline the proper disposal of media (physical or electronic) at *[Agency Name]*. These rules are in place to protect sensitive and classified information, employees and *[Agency Name]*. Inappropriate disposal of *[Agency Name]* and FBI Criminal Justice Information (CJI) and media may put employees, *[Agency Name]* and the FBI at risk.

### 2.0 Scope

This policy applies to all *[Agency Name]* employees, contractors, temporary staff, and other workers at *[Agency Name]*, with access to FBI CJIS systems and/or data, sensitive and classified data, and media. This policy applies to all equipment that processes, stores, and/or transmits FBI CJI and classified and sensitive data that is owned or leased by *[Agency Name]*.

### 3.0 Policy

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store and/or transmit FBI CJI and classified and sensitive data shall be properly disposed of in accordance with measures established by *[Agency Name]*.

Physical media (print-outs and other physical media) shall be disposed of by one of the following methods:

- 1) shredding using *[Agency Name]* issued shredders.
- 2) placed in locked shredding bins for *[private contractor name]* to come on-site and shred, witnessed by *[Agency Name]* personnel throughout the entire process.
- 3) incineration using *[Agency Name]* incinerators or witnessed by *[Agency Name]* personnel onsite at agency or at contractor incineration site, if conducted by non-authorized personnel.

Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier Hard-drives, etc.) shall be disposed of by one of the <Agency Name> methods:

- 1) **Overwriting (at least 3 times)** - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.
- 2) **Degaussing** - a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.
- 3) **Destruction** – a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc.,

ensuring that the platters have been physically destroyed so that no data can be pulled.

IT systems that have been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall not be released from *[Agency Name]*'s control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

#### **4.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination.

## **Information Technology Policy**

### **POLICY 604-01: CYBER SECURITY INCIDENT RESPONSE**

An incident, as defined in National Institute of Standards and Technology (NIST) Special Publication 800-61, is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

#### **OBJECTIVE:**

Ensure theis prepared to respond to cyber security incidents, to protect State systems and data, and prevent disruption of government services by providing the required controls for incident handling, reporting, and monitoring, as well as incident response training, testing, and assistance.

#### **SCOPE:**

This policy applies to all Executive Branch agencies, boards, and commissions except those exempt under The Code of

#### **RESPONSIBILITIES:**

##### **Individual Information Technology User:**

All users of State of\_\_\_\_\_ computing resources shall be aware of what constitutes a cyber security incident and shall understand incident reporting procedures.

##### **Information Services Division (ISD):**

Provide incident response support resources that offer advice and assistance with handling and reporting of security incidents for users of ISD information systems. Incident response support resources may include, for example, the ISD Help Desk, a response team (described below), and access to forensics services.

Establish a Cyber Security Incident Response Team (CSIRT) to ensure appropriate response to cyber security incidents. The CSIRT shall consist of members of the State IT Security Council and key personnel from other agencies as required. CSIRT responsibilities shall be defined in the Cyber Security Incident Reporting Procedures.

##### **Agency Management, Information Technology Organization:**

Develop organization and system-level cyber security incident response procedures to ensure management and key personnel are notified of cyber security incidents as required.

Organizations that support information systems shall develop incident response plans and/or procedures that:

- Provides the organization with a roadmap for implementing its incident response capability
- Describes the structure and organization of the incident response capability

- Provides a high-level approach for how the incident response capability fits into the overall organization
- Meets the unique requirements of the organization, which relate to mission, size, structure, and functions
- Defines reportable incidents
- Provides metrics for measuring the incident response capability within the organization
- Defines the resources and management support needed to effectively maintain and mature an incident response capability
- Is reviewed and approved by designated officials within the organization Review incident response plans and procedures at least annually.

Revise the incident response plan/procedures to address system/organizational changes or problems encountered during implementation, execution, or testing.

Distribute copies of the incident response plan/procedures to incident response personnel.

Communicate incident response plan/procedure changes to incident response personnel and other organizational elements as needed.

Provide incident response training to information system users consistent with assigned roles and responsibilities before authorizing access to the information system or performing assigned duties, when required by information system changes; and annually thereafter.

Organizations shall test the incident response capability for the information systems they support at least annually. Use organization-defined tests and/or exercises to determine incident response effectiveness. Document the results.

Organizations that support information systems shall implement an incident handling capability for cyber security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

Coordinate incident handling activities with contingency planning activities.

Incorporate the lessons learned from prior and ongoing incident handling activities into incident response procedures, training, and testing/exercises.

Track and document information system security incidents. Retain and safeguard cyber security incident documentation as evidence for investigation, corrective actions, potential disciplinary actions, and/or prosecution.

Promptly report cyber security incident information to appropriate authorities in accordance with State or organization incident reporting procedures.

Organizations that support information systems shall provide an incident response support resource integral to the organizational incident response capability that offers advice and assistance to users of the information

system for the handling and reporting of security incidents.

Possible implementations of incident response support resources in an organization include a help desk or an assistance group and, when required, access to forensics services.

**ADDITIONAL INFORMATION:**

Information Technology Procedure 604P1: Cyber Security Incident Reporting

[http://cybersecurity.alabama.gov/documents/Procedure 604P1 Incident Reporting.pdf](http://cybersecurity.alabama.gov/documents/Procedure_604P1_Incident_Reporting.pdf)

Information Technology Procedure 604P2: Cyber Security Incident Handling

[http://cybersecurity.alabama.gov/documents/Procedure 604P2 Incident Handling.pdf](http://cybersecurity.alabama.gov/documents/Procedure_604P2_Incident_Handling.pdf)

Information Technology Dictionary [http://cybersecurity.alabama.gov/documents/IT Dictionary.pdf](http://cybersecurity.alabama.gov/documents/IT_Dictionary.pdf)

*By Authority of Director, Information Services Division, Department of Finance*

**DOCUMENT HISTORY:**

Version	Release Date	Comments
604-00	06/16/2011	Combines and replaces Policy 600-04 and Standard 600-04S1
604-01	07/19/2012	Reorganized requirements under Agency Responsibilities, and updated consistent with NIST 800-53 and 800-61 guidance

Policy Title:	Media Protection Policy
Effective Date:	
Revision Date:	Every 2 years or as needed
Approval(s):	
LASO:	
CSO:	
Agency Head:	

**Purpose:**

The intent of the Media Protection Policy is to ensure the protection of the Criminal Justice Information (CJI) until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules.

This Media Protection Policy was developed using the FBI’s Criminal Justice Information Services (CJIS) Security Policy 5.1 dated 7/13/2012. The *[agency name]* may complement this policy with a local policy; however, the CJIS Security Policy shall always be the minimum standard. The local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

**Scope:**

The scope of this policy applies to any electronic or physical media containing FBI Criminal Justice Information (CJI) while being stored, accessed or physically moved from a secure location from the *[agency name]*. This policy applies to any authorized person who accesses, stores, and / or transports electronic or physical media. Transporting CJI outside the agency’s assigned physically secure area must be monitored and controlled.

Authorized *[agency name]* personnel shall protect and control electronic and physical CJI while at rest and in transit. The *[agency name]* will take appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate CJI disclosure and/or use will be reported to the *[agency name]* Local Agency Security Officer (LASO). Procedures shall be defined for securely handling, transporting and storing media.

**Media Storage and Access:**

Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored, or actively being accessed. “Electronic media” includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. “Physical media” includes printed documents and imagery that contain CJI.

To protect CJI, the *[agency name]* personnel shall:

1. Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room.
2. Restrict access to electronic and physical media to authorized individuals.
3. Ensure that only authorized users remove printed form or digital media from the CJI.
4. Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using approved equipment, techniques and procedures. (See Sanitization Destruction Policy)
5. Not use personally owned information system to access, process, store, or transmit CJI unless the *[agency name]* has established and documented the specific terms and conditions for personally owned information system usage. (See Personally Owned Device Policy)
6. Not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
7. Store all hardcopy CJI printouts maintained by the *[agency name]* in a secure area accessible to only those employees whose job function require them to handle such documents.
8. Safeguard all CJI by the *[agency name]* against possible misuse by complying with the Physical Protection Policy, Personally Owned Device Policy, and Disciplinary Policy.
9. Take appropriate action when in possession of CJI while not in a secure area:
  - a. CJI must not leave the employee's immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.
  - b. Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock use and /or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption.
    - i. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, back---up tapes, mobile devices, laptops, etc.
    - ii. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140---2 standards.
10. Lock or log off computer when not in immediate vicinity of work area to protect CJI. Not all personnel have same CJI access permissions and need to keep CJI protected on a need---to---know basis.

11. Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of CJI. (See Physical Protection Policy)

### **Media Transport:**

Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. "Electronic media" means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

Dissemination to another agency is authorized if:

1. The other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or
2. The other agency is performing personnel and appointment functions for criminal justice employment applicants.

The *[agency name]* personnel shall:

1. Protect and control electronic and physical media during transport outside of controlled areas.
2. Restrict the pickup, receipt, transfer and delivery of such media to authorized personnel.

The *[agency name]* personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:

1. Use of privacy statements in electronic and paper documents.
2. Limiting the collection, disclosure, sharing and use of CJI.
3. Following the least privilege and role based rules for allowing access.  
Limit access to CJI to only those people or roles that require access.
4. Securing hand carried confidential electronic and paper documents by:
  - a. Storing CJI in a locked briefcase or lockbox.
  - b. Only viewing or accessing the CJI electronically or document printouts in a physically secure location by authorized personnel.
  - c. For hard copy printouts or CJI documents:
    - i. Package hard copy printouts in such a way as to not have any CJI information viewable.
    - ii. That are mailed or shipped, agency must document procedures and only release to authorized individuals. **DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL.** Packages containing CJI material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery. (Agency Discretion)
5. Not taking CJI home or when traveling unless authorized by *[agency name]* LASO. When disposing confidential documents, use a shredder.

### **Electronic Media Sanitization and Disposal:**

The agency shall sanitize, that is, overwrite at least three times or degauss electronic media 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 sanitization or destruction is witnessed or carried out by authorized personnel. Physical media shall be securely disposed of when no longer required, using formal procedures. For end of life media policy, refer to “Sanitization Destruction Policy”.

### **Breach Notification and Incident Reporting:**

The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

### **Roles and Responsibilities:**

If CJI is improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:

1. *[agency name]* personnel shall notify his/her supervisor or LASO, and an incident---report form must be completed and submitted within 24 hours of discovery of the incident. The submitted report is to contain a detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident. (Agency Discretion)
2. The supervisor will communicate the situation to the LASO to notify of the loss or disclosure of CJI records.
3. The LASO will ensure the CSA ISO (CJIS System Agency Information Security Officer) is promptly informed of security incidents.
4. The CSA ISO will:
  - a. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.
  - b. Collect and disseminate all incident---related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
  - c. Act as a single POC for their jurisdictional area for requesting incident response assistance.

### **Penalties:**

Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and / or termination.

**Acknowledgement:**

I have read the policy and rules above and I will:

- Abide by the *[agency name]*'s Media Protection Policy. I understand any violation of this policy may result in discipline up to and including termination.
- Report any *[agency name]* CJI security incident to Supervisor and / or LASO as identified in this policy.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_/2012\_\_\_\_\_

**Questions**

Any questions related to this policy may be directed to the *[agency name]*'s LASO:

LASO Name:	LASO Phone:	LASO email:
State C/ISO Name:	C/ISO Phone:	C/ISO email:

Policy Title:	Allowed Personally Owned Device Policy
Effective Date:	
Revision Date:	Every 2 years or as needed
Approval(s):	
LASO:	
CSO:	
Agency Head:	

**Purpose:**

A personally owned information system or device shall be authorized to access, process, store or transmit [agency name], state, or FBI Criminal Justice Information (CJI) only when these established and documented specific terms and conditions are met. This control does not apply to the use of personally owned information systems to access the [agency name]'s information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).

This Personally Owned Device Policy was developed using the FBI's *CJIS Security Policy* 5.1 dated July 13, 2012. The intended target audience is [agency name] personnel, support personnel and private contractors/vendors. The [agency name] may complement this policy with a local policy; however, the *CJIS Security Policy* shall always be the minimum standard and the local policy may augment, or increase the standards, but shall not detract from the *CJIS Security Policy* standards.

**Scope:**

This policy applies to all [agency name] personnel, support personnel, and/or private contractors/vendors who are authorized to use personally owned devices to connect to any physical, logical, and/or electronic premise of the [agency name] to access, process, store, and/or transmit CJI. This also includes any private contractors/vendors who will conduct maintenance on any network device that processes, stores, and/or transmits FBI CJI.

**Personally Owned Devices:**

A personally owned device is any technology device that was purchased by an individual and was not issued by the [agency name]. A personal device includes any portable technology like camera, USB flash drives, USB thumb drives, DVDs, CDs, air cards and mobile wireless devices such as Androids, Blackberry OS, Apple iOS, Windows Mobile, Symbian, tablets, laptops or any personal desktop computer. Threats to mobile handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services.

The [agency name] will maintain management control and authorize the use of personally owned devices. The [agency name] shall develop guidelines to define which employees can use their own devices, the types of devices they can use, and which applications and data they can access, process, or store on their devices.

Personally owned devices must:

- Be authorized by [agency name] to access, process, transmit, and/or store FBI CJI.
- Be inspected by [agency name]'s IT staff and the LASO to ensure appropriate security requirements on the device are up-to-date and meet the FBI's *CJIS Security Policy* requirements prior to use.
- Take necessary precautions when using device outside of a physically secure area. Read below and also see Physical Protection Policy.

#### **Remote Access:**

The [agency name] shall authorize, monitor, and control all methods of remote access to the information systems that can access, process, transmit, and/or store FBI CJI. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency controlled network (e.g., the Internet).

The [agency name] shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The [agency name] shall control all remote accesses through managed access control points. The [agency name] may permit remote access for privileged functions only for compelling operational needs but shall document the rationale for such access in the security plan for the information system.

Utilizing publicly accessible computers to access, process, store or transmit CJI is prohibited. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

#### **Roles and Responsibilities:**

**Owner Role:** The owner agrees to:

1. Follow necessary policy and procedures to protect FBI CJI.
2. Usage of their device will be for work-related purposes.
3. Bring their device to work to use during normal work hours and not share the device with anyone else.
4. [agency name] having the authority to erase device remotely as needed.
5. Be responsible for any financial obligations for device.
6. Protect individual's and [agency name]'s privacy.
7. Use good judgement before installing free applications. Sometimes free applications track your personal information with limited disclosure or authorization, and then sell your profile to advertising companies.
8. Use good judgement on amount of time applied to personal use of personally owned devices during normal work business hours.
9. Access FBI CJI only from an approved and authorized storage device.
10. Do not stream music or videos using personally owned devices when connected to [agency name]'s network to prevent sluggishness.

11. Report lost or stolen mobile or storage devices to the [agency name]'s Local Agency Security Officer (LASO) within one business day.
12. Review the use of device alerts and update services to validate you requested them. Restrict notifications not requested by looking at your device's settings.
13. Control wireless network and service connectivity. Validate mobile device default settings are not connecting to nearby Wi-Fi networks automatically. Some of these networks, like in airports or neighborhood coffee shops, may be completely open and unsecure.

### **Information Technology Role**

The [agency name] IT support role shall, at a minimum, ensure that external storage devices:

1. Are encrypted when FBI CJI is stored electronically.
2. Are scanned for virus and malware prior to use and/or prior to being connected to the agency's computer or laptop.

The [agency name] IT support role shall, at a minimum, ensure that all personally owned devices:

1. Apply available critical patches and upgrades to the device operating system.
2. Are kept updated with security patches, firmware updates and antivirus.
3. Are configured for local device authentication.
4. Use advanced authentication and encryption when FBI CJI is stored and/or transmitted.
5. Be able to deliver built-in identity role-mapping, network access control (NAC), AAA (Authentication, Authorization, and Accounting) services, and real-time endpoint reporting.
6. Erase cached information when session is terminated.
7. Employ personal firewalls.
8. Minimize security risks by ensuring antivirus and antimalware are installed, running real time and updated.
9. Be scanned for viruses and malware prior to accessing or connecting to [agency name] CJIS network.
10. Configure Bluetooth interface as undiscoverable except as needed for pairing, which prevents visibility to other Bluetooth devices except when discovery is specifically needed.
11. Be properly disposed of at end of life. See Media Disposal Policy. Remove FBI CJI before owner sells their personally owned devices or sends it in for repairs.
12. Evaluate personally owned device age. Older device hardware is too outdated for needed updates. Typical life is two years.
13. Ensure device is compatible with needed network protocols and/or compatible with customized applications developed for access FBI CJI through testing.
14. Deploy Mobile Device Management or SIM card locks and credential functions. The credential functions require a pass code to use [agency name]'s network services. *(Research enterprise mobile device management solutions-- see product working successfully in real life scenario with the type of mobile device your*

*State/Agency wants to use prior to implementing. The enterprise mobile device solution must be compatible with chosen device products.)*

15. Ensure owner and IT staff have mobile backup enabled to an approved [agency name] location. Set a daily or weekly schedule to periodically synch data and applications. If backup contains FBI CJI, take appropriate security measures for storage of FBI CJI. See Media Protection Policy.
16. Retain the ability to secure, control and remotely erase agency data on employee---owned devices in the event of a security breach or if the employee leaves the agency employment or the device is lost or stolen. This remote ability can be done through technology that allows virtual access to company applications.
17. Enable mobile device in a “find my phone” service to allow finding device.
18. Consider adding extra protection such as a total device reset if the PIN is guessed incorrectly a certain number of attempts.
19. Be able to easily identify connected users and devices. Track, log and manage every personally used device allowed to connect to agency technology resources for secure FBI CJI access.
20. Perform pre and post---authentication checks.
21. Ability to allow and deny access. Selectively grant proper network access privileges.

### **Local Area Security Officer (LASO)**

The LASO will:

1. Identify who is using the personally owned approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

### **Penalties:**

Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and/or termination. Personally owned information technology resources used may be retained by the [agency name] for evaluation in investigation of security violations.

Violation of any of the requirements in this policy by any unauthorized person can result in similar disciplinary action against the device owner, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

**Acknowledgement:**

The [agency name], agency personnel, IT support, private contractors/vendors, and the LASO alike will agree to commit to all bring your own (BYO) rules.

I have read the policy and rules above and I will:

- Authorize the [agency name] to remotely wipe my mobile device.
- Abide by the [agency name] Personally Owned Device policy. I understand any violation of this policy may result in discipline up to and including termination.
- Complete the security awareness training and take action to protect [agency name] facilities, personnel and associated information systems.
- Report any unauthorized device access to [agency name] LASO.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_/20\_\_\_\_\_

**Questions**

Any questions related to this policy may be directed to the [agency name]'s LASO:

LASO Name:	LASO Phone:	LASO email:
State CSO/ISO Name:	CSO/ISO Phone:	CSO/ISO email:

Other Related Policy Reference:

- See Media Sanitization and Destruction Policy
- Physical Protection Policy

Policy Title:	Physical Protection Policy
Effective Date:	
Revision Date:	Every 2 years or as needed
Subject Matter Experts / Approval(s):	
TAC:	
LASO:	
C/ISO:	
Front Desk:	
Technology Support Lead:	
Agency Head:	

**Purpose:**

The purpose of this policy is to provide guidance for agency personnel, support personnel, and private contractors/vendors for the physical, logical, and electronic protection of Criminal Justice Information (CJI). All physical, logical, and electronic access must be properly documented, authorized and controlled on devices that store, process, or transmit unencrypted CJI. This Physical Protection Policy focuses on the appropriate access control methods needed to protect the full lifecycle of CJI from insider and outsider threats.

This Physical Protection Policy was developed using the FBI’s *CJIS Security Policy 5.1* dated July 13, 2012. The intended target audience is [agency name] personnel, support personnel, and private contractor/vendors with access to CJI whether logically or physically. The local agency may complement this policy with a local policy; however, the *CJIS Security Policy* shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the *CJIS Security Policy* standards.

**Physically Secure Location:**

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 the FBI CJI and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non---secure locations by physical controls. Security perimeters shall be defined, controlled, and secured. Restricted non---public areas in the [agency name] shall be identified with a sign at the entrance.

**Visitors Access:**

A visitor is defined as a person who visits the [agency name] facility on a temporary basis who is not employed by the [agency name] and has no unescorted access to the physically secure location within the [agency name] where FBI CJI and associated information systems are located. For agencies with jails with CJIS terminals, additional visit specifications need to be established per agency purview and approval.

Visitors shall:

1. Check in before entering a physically secure location by:
  - a. Completing the visitor access log, which includes: name and visitor's agency, purpose for the visit, date of visit, time of arrival and departure, name and agency of person visited, and form of identification used to authenticate visitor.
  - b. Document badge number on visitor log if visitor badge issued. If [agency name] issues visitor badges, the visitor badge shall be worn on approved visitor's outer clothing and collected by the agency at the end of the visit.
  - c. Planning to check or sign-in multiple times if visiting multiple physically secured locations and/or building facilities that are not adjacent or bordering each other that each has their own individual perimeter security to protect CJI.
2. Be accompanied by a [agency name] escort at all times to include delivery or service personnel. An escort is defined as an authorized personnel who accompanies a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any CJI therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.
3. Show [agency name] personnel a valid form of photo identification.
4. Follow [agency name] policy for authorized unescorted access.
  - a. Noncriminal Justice Agency (NCJA) like city or county IT who require frequent unescorted access to restricted area(s) will be required to establish a Management Control Agreement between the [agency name] and NCJA. Each NCJA employee with CJI access will appropriately have state and national fingerprint--based record background check prior to this restricted area access being granted.
  - b. Private contractors/vendors who requires frequent unescorted access to restricted area(s) will be required to establish a Security Addendum between the [agency name] and each private contractor personnel. Each private contractor personnel will appropriately have state and national fingerprint---based record background check prior to this restricted area access being granted.
5. Not be allowed to view screen information mitigating shoulder surfing.
6. Individuals not having any legitimate business in a restricted area shall be courteously escorted to a public area of the facility. Strangers in physically secure areas without an escort should be challenged. If resistance or behavior of a threatening or suspicious nature is encountered, sworn personnel shall be notified or call 911.
7. Not be allowed to sponsor another visitor.
8. Not enter into a secure area with electronic devices unless approved by the [agency name] Local Area Security Officer (LASO) to include cameras and mobile devices. Photographs are not allowed without permission of the [agency name] assigned personnel.
9. All requests by groups for tours of the [agency name] facility will be referred to the proper agency point of contact for scheduling. In most cases, these groups will be handled by a single form, to be signed by a designated group leader or representative. Remaining visitor rules apply for each visitor within the group. The group leader will provide a list of names to front desk personnel for instances of emergency evacuation and accountability of each visitor while on agency premises.

### Authorized Physical Access:

Only authorized personnel will have access to physically secure non---public locations. The [agency name] will maintain and keep current a list of authorized personnel. All physical access points into the agency's secure areas will be authorized before granting access. The agency will implement access controls and monitoring of physically secure areas for protecting all transmission and display mediums of CJI. Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches.

All personnel with CJI physical and logical access must:

1. Meet the minimum personnel screening requirements prior to CJI access.
  - a. To verify identification, a state of residency and national fingerprint---based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.
  - b. Support personnel, private contractors/vendors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint---based record check unless these individuals are escorted by authorized personnel at all times.
  - c. Prior to granting access to CJI, the [agency name] on whose behalf the contractor is retained shall verify identification via a state of residency and national fingerprint---based record check.
  - d. Refer to the *CJIS Security Policy* for handling cases of felony convictions, criminal records, arrest histories, etc.
2. Complete security awareness training.
  - a. All authorized [agency name], Noncriminal Justice Agencies (NCJA) like city or county IT and private contractor/vendor personnel will receive security awareness training within six months of being granted duties that require CJI access and every two years thereafter.
  - b. Security awareness training will cover areas specified in the *CJIS Security Policy* at a minimum.
3. Be aware of who is in their secure area before accessing confidential data.
  - a. Take appropriate action to protect all confidential data.
  - b. Protect all terminal monitors with viewable CJI displayed on monitor and not allow viewing by the public or escorted visitors.
4. Properly protect and not share any individually issued keys, proximity cards, computer account passwords, etc.
  - a. Report loss of issued keys, proximity cards, etc to authorized agency personnel.
  - b. If the loss occurs after normal business hours, or on weekends or holidays, personnel are to call the [agency name] POC to have authorized credentials like a proximity card de---activated and/or door locks possibly rekeyed.
  - c. Safeguard and not share passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and all other facility and computer systems security access procedures. See Disciplinary Policy.
5. Properly protect from viruses, worms, Trojan horses, and other malicious code.

6. Web usage—allowed versus prohibited; monitoring of user activity. (allowed versus prohibited is at the agency’s discretion)
7. Do not use personally owned devices on the [agency name] computers with CJI access. (Agency discretion). See Personally Owned Policy.
8. Use of electronic media is allowed only by authorized [agency name] personnel. Controls shall be in place to protect electronic media and printouts containing CJI while in transport. When CJI is physically moved from a secure location to a non---secure location, appropriate controls will prevent data compromise and/or unauthorized access.
9. Encrypt emails when electronic mail is allowed to transmit CJI---related data as such in the case of Information Exchange Agreements.
  - a. (Agency Discretion for allowance of CJI via email)
  - b. If CJI is transmitted by email, the email must be encrypted and email recipient must be authorized to receive and view CJI.
10. Report any physical security incidents to the [agency name]’sLASO to include facility access violations, loss of CJI, loss of laptops, Blackberries, thumb drives, CDs/DVDs and printouts containing CJI.
11. Properly release hard copy printouts of CJI only to authorized vetted and authorized personnel in a secure envelope and shred or burn hard copy printouts when no longer needed. Information should be shared on a “need to know” basis. (See Sanitization and Destruction Policy)
12. Ensure data centers with CJI are physically and logically secure.
13. Keep appropriate [agency name] security personnel informed when CJI access is no longer needed. In the event of ended employment, the individual must surrender all property and access managed by the local agency, state and/or federal agencies.
14. Not use food or drink around information technology equipment.
15. Know which door to use for proper entry and exit of the [agency name] and only use marked alarmed fire exits in emergency situations.
16. Ensure the perimeter security door securely locks after entry or departure. Do not leave any perimeter door propped opened and take measures to prevent piggybacking entries.

### **Roles and Responsibilities:**

#### **Terminal Agency Coordinator (TAC)**

The TAC serves as the point---of---contact at the [agency name] for matters relating to CJIS information access. The TAC administers CJIS systems programs within the agency and oversees the agency’s compliance with FBI and state CJIS systems policies.

#### **Local Agency Security Officer (LASO)**

Each LASO shall:

1. Identify who is using the CSA (state) approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

### **Agency Coordinator (AC)**

An AC is a staff member of the Contracting Government Agency (CGA) who manages the agreement between the private contractor(s)/vendor(s) and the [agency name]. A CGA is a government agency, whether a Criminal Justice Agency (CJA) or a NCJA, that enters into an agreement with a private contractor/vendor subject to the CJIS Security Addendum. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of private contractor/vendor employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC.

### **CJIS System Agency Information Security Officer (CSA ISO)**

The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.
2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.
3. Document and provide assistance for implementing the security---related controls for the Interface Agency and its users.
4. ISOs have been identified as the POC on security---related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

### **Information Technology Support**

In coordination with above roles, all vetted IT support staff will protect CJI from compromise at the [agency name] by performing the following:

1. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed. Know where CJI is stored, printed, copied, transmitted and planned end of life. CJI is stored on laptops, mobile data terminals (MDTs), computers, servers, tape backups, CDs, DVDs, thumb drives, RISC devices and internet connections as authorized by the [agency name]. For agencies who submit fingerprints using Live Scan terminals, only Live Scan terminals that receive CJI back to the Live Scan terminal will be assessed for physical security.
2. Be knowledgeable of required [agency name] technical requirements and policies taking appropriate preventative measures and corrective actions to protect CJI at rest, in transit and at the end of life.
3. Take appropriate action to ensure maximum uptime of CJI and expedited backup restores by using agency approved best practices for power backup and data backup means such as generators, backup universal power supplies on CJI---based terminals, servers, switches, etc.
4. Properly protect the [agency name]'s CJIS system(s) from viruses, worms, Trojan horses, and other malicious code (real---time scanning and ensure updated definitions).
  - a. Install and update antivirus on computers, laptops, MDTs, servers, etc.

- b. Scan any outside non---agency owned CDs, DVDs, thumb drives, etc., for viruses, if the [agency name] allows the use of personally owned devices. (See the [agency name] Personally Owned Device Policy)
- 5. Data backup and storage—centralized or decentralized approach.
  - a. Perform data backups and take appropriate measures to protect all stored CJI.
  - b. Ensure only authorized vetted personnel transport off---site tape backups or any other media that store CJI that is removed from physically secured location.
  - c. Ensure any media released from the [agency name] is properly sanitized / destroyed. (See Sanitization and Destruction Policy)
- 6. Timely application of system patches—part of configuration management.
  - a. The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.
  - b. When applicable, see the [agency name] Patch Management Policy.
- 7. Access control measures
  - a. Address least privilege and separation of duties.
  - b. Enable event logging of:
    - i. Successful and unsuccessful system log---on attempts.
    - ii. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.
    - iii. Successful and unsuccessful attempts to change account passwords.
    - iv. Successful and unsuccessful actions by privileged accounts.
    - v. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.
  - c. Prevent authorized users from utilizing publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
- 8. Account Management in coordination with TAC
  - a. Agencies shall ensure that all user IDs belong to currently authorized users.
  - b. Keep login access current, updated and monitored. Remove or disable terminated or transferred or associated accounts.
  - c. Authenticate verified users as uniquely identified.
  - d. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs.
  - e. Not use shared generic or default administrative user accounts or passwords for any device used with CJI.
  - f. Passwords
    - i. Be a minimum length of eight (8) characters on all systems.
    - ii. Not be a dictionary word or proper name.
    - iii. Not be the same as the Userid.
    - iv. Expire within a maximum of 90 calendar days.

- v. Not be identical to the previous ten (10) passwords.
  - vi. Not be transmitted in the clear or plaintext outside the secure location.
  - vii. Not be displayed when entered.
  - viii. Ensure passwords are only reset for authorized user.
9. Network infrastructure protection measures.
- a. Take action to protect CJI---related data from unauthorized public access.
  - b. Control access, monitor, enabling and updating configurations of boundary protection firewalls.
  - c. Enable and update personal firewall on mobile devices as needed.
  - d. Ensure confidential electronic data is only transmitted on secure network channels using encryption and \*advanced authentication when leaving a physically secure location. No confidential data should be transmitted in clear text. *\*Note: for interim compliance, and for the sole purpose of meeting the advanced authentication policy, a police vehicle shall be considered a physically secure location until September 30th 2013. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods.*
  - e. Ensure any media that is removed from a physically secured location is encrypted in transit by a person or network.
  - f. Not use default accounts on network equipment that passes CJI like switches, routers, firewalls.
  - g. Make sure law enforcement networks with CJI shall be on their own network accessible by authorized personnel who have been vetted by the [agency name]. Utilize Virtual Local Area Network (VLAN) technology to segment CJI traffic from other noncriminal justice agency traffic to include other city and/or county agencies using same wide area network.
10. Communicate and keep the [agency name] informed of all scheduled and unscheduled network and computer downtimes, all security incidents and misuse. The ultimate information technology management control belongs to [agency name].

### **Front desk and Visitor Sponsoring Personnel**

Administration of the Visitor Check---In / Check---Out procedure is the responsibility of identified individuals in each facility. In most facilities, this duty is done by the Front desk or Reception Desk.

Prior to visitor gaining access to physically secure area:

1. The visitor will be screened by the [agency name] personnel for weapons. No weapons are allowed in the agency except when carried by authorized personnel as deemed authorized by the [agency name].
2. The visitor will be screened for electronic devices. No personal electronic devices are allowed in any agency facility except when carried by authorized personnel as deemed authorized by the [agency name].
3. Escort personnel will acknowledge being responsible for properly evacuating visitor in cases of emergency. Escort personnel will know appropriate evacuation

routes and procedures.

4. Escort and/or Front desk personnel will validate visitor is not leaving agency with any agency owned equipment or sensitive data prior to Visitor departure.

All [agency name] personnel and supporting entities are responsible to report any unauthorized physical, logical, and electronic access to the [agency name] officials. For [agency name], the point of contacts to report any non--secure access is:

LASO Name:	LASO Phone:	LASO email:
AC Name:	AC Phone:	AC email:
State C/ISO Name:	C/ISO Phone:	C/ISO email:

**Penalties:**

Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and / or termination.

Violation of any of the requirements in this policy by any visitor can result in similar disciplinary action against the sponsoring employee, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

**Acknowledgement:**

I have read the policy and rules above and I will:

- Abide by the [agency name] Physical Protection Policy. I understand any violation of this policy may result in discipline up to and including termination.
- Complete the security awareness training and take action to protect the [agency name]'s facilities, personnel and associated information systems.
- Report any unauthorized physical access to the [agency name]'s LASO.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_/2012\_

Other Related Policy Reference:

- Sanitization and Destruction Policy
- Disciplinary Policy
- *CJIS Security Policy*

## **User Rules of Behavior Acknowledgment Form**

As a user of an IT system, I acknowledge my responsibility to conform to the following requirements and conditions as directed by all relevant Information Assurance and Information Security Policies, Procedures and Guidelines. These conditions apply to all personnel who have access to FBI CJIS systems and all appropriate IT personnel.

1. I understand that failure to sign this acknowledgment will result in denial of access to FBI CJIS systems, terminal areas, and facilities that have FBI CJIS network equipment.
2. I acknowledge my responsibility to use the network only for official business except for such personal use involving negligible cost to the agency and no interference with official business as may be permissible under the acceptable use policy.
3. I understand that the network operates at a Sensitive but Unclassified level. I have all clearance necessary for access to the network, and will not introduce or process data that the network is not specifically designed to handle as specified by the Security Policy.
4. I understand the need to protect my password at the highest level of data it secures. I will NOT share my password and/or account. I understand that neither the Security Administrator/System Administrator, nor the Network Operations Center (NOC) will request my password. I will change my password at least every 90 days or as requested for security reasons.
5. I understand I am responsible for all actions taken under my account. I will not attempt to “hack” the network or any connected automated information system (AIS), or attempt to gain access to data for which I am not specifically authorized.
6. I understand my responsibility to appropriately protect all output generated under my account, to include printed material, magnetic tapes, floppy disks, CD-ROMs, and downloaded hard disk files. I understand that I am required to ensure all hard copy material and magnetic media is properly labeled as required by policies and regulations.
7. I understand my responsibility to report all AIS or network problems to my security point of contact. I will NOT install, remove, or modify any hardware or software.
8. I acknowledge my responsibility to not introduce any software or hardware not acquired and approved through the IT Security group. I also acknowledge my

responsibility to have all official electronic media virus-scanned by the IT Security group before introducing it into the AIS or network.

9. I acknowledge my responsibility to conform to the requirements of the Rules of Behavior, Acceptable Use Policy, and Security Policies and Procedures. I also acknowledge that failure to comply with these policies and procedures may constitute a security violation resulting in denial of access to the AIS, network, or facilities, and that such violations will be reported to appropriate authorities for further actions as deemed appropriate to include disciplinary, civil, or criminal penalties.
10. I agree that I have no expectation of privacy in any equipment or media I use. I consent to inspections by authorized agency personnel, at any time and agree to make any equipment available for audit and review by FBI personnel upon request.
11. I further consent that my use of FBI CJIS systems within agency owned or leased space is subject to system monitoring.
12. I have completed the required triennial Security Awareness Training required by the *CJIS Security Policy* for individuals managing or accessing FBI CJIS systems and/or data.

**User (Print Name):** \_\_\_\_\_ **Date:** \_\_\_\_\_

**User Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_

**ISO/Security Officer:** \_\_\_\_\_ **Date:** \_\_\_\_\_

Policy Title:	User Account / Access Validation Policy
Effective Date:	
Revision Date:	Every 2 years or as needed
Subject Matter Experts / Approval(s):	
TAC:	
LASO:	
C/ISO:	
Front Desk:	
Technology Support Lead:	
Agency Head:	

**Purpose:**

All accounts shall be reviewed at least every six months by the terminal agency coordinator (TAC) or his/her designee to ensure that access and account privileges commensurate with job functions, need-to-know, and employment status on systems that contain Criminal Justice Information. The TAC may also conduct periodic reviews.

All guest accounts (for those who are not official employees of the CJA) with access to the criminal justice network shall contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts (for private contractor personnel) must be sponsored by the appropriate authorized member of the administrative entity managing the resource.

The TAC must disable all new accounts that have not been accessed within 30 days of creation. Accounts of individuals on extended leave (more than 30 days) should be disabled. (Note: Exceptions can be made in cases where uninterrupted access to IT resources is required. In those instances, the individual going on extended leave must have a manager-approved request from the designated account administrator or assistant.)

The TAC must be notified if a user's information system usage or need-to-know changes (i.e., the employee is terminated, transferred, etc.). If an individual is assigned to another office for an extended period (more than 90 days), the TAC will transfer the individual's account(s) to the new office (CJA).

The TAC will remove or disable all access accounts for separated or terminated employees immediately following separation from the agency.

Primary responsibility for account management belongs to the Terminal Agency Coordinator (TAC). The TAC shall:

- Modify user accounts in response to events like name changes, accounting changes, permission changes, office transfers, etc.,
- Periodically review existing accounts for validity (at least once every 6 months), and
- Cooperate fully with an authorized security team that is investigating a security incident or performing an audit review.

**F.1 Security Incident Response Form**

**FBI CJIS DIVISION  
INFORMATION SECURITY  
OFFICER (ISO) SECURITY  
INCIDENT REPORTING FORM**

---

NAME OF PERSON REPORTING THE INCIDENT: \_\_\_\_\_

DATE OF REPORT: \_\_\_\_\_ (mm/dd/yyyy)

DATE OF INCIDENT: \_\_\_\_\_ (mm/dd/yyyy)

POINT(S) OF CONTACT (Include Phone/Extension/Email): \_\_\_\_\_

LOCATION(S) OF INCIDENT: \_\_\_\_\_

INCIDENT DESCRIPTION: \_\_\_\_\_

SYSTEM(S) AFFECTED: \_\_\_\_\_

SYSTEM(S) AFFECTED (e.g. CAD, RMS, file server, etc.): \_\_\_\_\_

METHOD OF DETECTION: \_\_\_\_\_

ACTIONS TAKEN/RESOLUTION: \_\_\_\_\_

**Copies To:**

[iso@nigc.gov](mailto:iso@nigc.gov)

**and**

**John C. Weatherly**

(FBI CJIS Division ISO) 1000

Custer Hollow Road

Clarksburg, WV 26306-0102

(304) 625-3660

[iso@fbi.gov](mailto:iso@fbi.gov)

## Appendix G

### LOCAL AGENCY SECURITY OFFICER (LASO) BASIC RESPONSIBILITIES

RESPONSIBILITY	DESCRIPTION
Primary liaison	<p>Person through which all communication regarding audits, training, and security is conducted.</p> <p>First point of contact for NIGC in the event of an allegation of criminal history misuse or a security issue involving the background check process.</p>
Information Changes	Keeps information with NIGC current by informing the NIGC of any changes in the Tribe's information, the LASO, or the Authorized Tribal Signatory (submits the proper information change forms).
Authorized Personnel List	Submits and maintains a current Authorized Personnel List with the NIGC.
Privacy and Security Compliance	<p>Primarily responsible for agency compliance with all Privacy and Security rules.</p> <p>Maintains copies of Authorized Personnel Acknowledgement Statements and dissemination logs (if applicable).</p> <p>Ensures Tribe has adequate policies/procedures related to access, use, handling, dissemination, and destruction of CJI/CHRI.</p>
Training	<p>Ensures Authorized Personnel receive required agency-provided privacy and security training. Reviews Tribal training outlines to ensure topics are adequately covered.</p> <p>Ensures Authorized Personnel receive required standard online training.</p> <p>Updates Tribe training documentation as needed.</p>
Audits	<p>Cooperates with NIGC and/or federal officials during the audit process.</p> <p>Maintains all required audit documentation and serves as the Tribal representative for audits.</p> <p>Completes all documentation required during the audit and submits any required corrective action documentation in a timely manner.</p>

And

ISO@NIGC.GOV

## Appendix H

### Sample Noncriminal Justice Agency Information Change Form

<b>Date</b>	<b>Agency Name</b>	<b>Agency ORI</b>
-------------	--------------------	-------------------

<b>Change/Add Contact Type:</b> Check all that apply  Local Agency Security Officer (LASO) <input type="checkbox"/>  Applicant Team <input type="checkbox"/>  Secondary LASO <input type="checkbox"/>	<i>Previous Contact</i>		
	<i>New Contact Information</i>		
	<b>Title</b>	<b>Name</b>	
	<b>Phone</b>	<b>Fax</b>	<b>Email</b>

<b>Change Authorized Tribal Signatory</b>	<i>Previous Authorized Tribal Signatory Name</i>		
	<i>New Authorized Tribal Signatory Information</i>		
	<b>Title</b>	<b>Name</b>	
	<b>Phone</b>	<b>Fax</b>	<b>Email</b>

<b>Change Address:</b> <input type="checkbox"/>  Physical <input type="checkbox"/>  Mailing <input type="checkbox"/>	<b>Address Line 1</b>		
	<b>Address Line 2</b>		
	<b>City</b>	<b>State</b>	<b>Zip</b>

<b>Change Agency Name</b> Previous Name:  New Name:	<b>Change Agency Main Phone</b> New phone number:
--	--

<b>Additional Comments/Information:</b>   	Leave Blank – NIGC use only
---	-----------------------------

Send completed form to:	National Indian Gaming Commission ATTN: Information Security Officer 1849 C Street NW   Mail Stop 1621 Washington, DC 20240	<b>OR</b>	Fax: (202-632-7066 ATTN: Information Security Officer  Email: iso@nigc.gov
-------------------------	---	-----------	---

# Appendix I

## Sample Authorized Personnel List

Name	Tribe Name	Commission or Casino Name	Department	Position	LASO Y/N	Email	Phone	Date Added	Date Termed
Jane Doe	AAA Tribe	XXX Gaming Commission	Licensing	Licensing Manager	Y	<a href="mailto:J.doe@abc.com">J.doe@abc.com</a>	555-555-5555	1/25/2020	
John Doe			Licensing	Background Investigator	N	<a href="mailto:Ddoe@xyz.com">Ddoe@xyz.com</a>		2/15/2020	
Bobby Smith			Commission	Commissioner	N	<a href="mailto:b.smith@abc.com">b.smith@abc.com</a>	444-444-4444	1/1/2018	2/25/2020
Dan Smith		Lucky Casino	IT	IT Manager	N	<a href="mailto:Dan@luckycasino.net">Dan@luckycasino.net</a>	123-45-6789	2/15/2020	

**Notes:**

- 1) Please list all Authorized Personnel who are authorized to receive, view, handle, disseminate, store, retrieve or dispose of CJ/CHRI. This includes having access to the fingerprint system.
- 2) Please document date an employee is no longer authorized to view/handle CJ/CHRI.
- 3) Please submit legal name changes and contact information updates if applicable.
- 4) If information is the same as the previous row, leave the information for the row blank

# SAMPLE

## ZYX Gaming Commission

123 Any Town Road  
Your Town, AB 12345

May 1, 2020

National Indian Gaming Commission  
1849 C Street NW  
Mail Stop #1621  
Washington, DC 20240

Dear NIGC Information Security Officer:

The following is an updated authorized personnel list for the ZYX Gaming Commission.

<u>Authorized Individual</u>	<u>Title</u>
Smith, John	Commissioner
Doe, Jane	Executive Director
Anderson, Sandy	Licensing Manager (LASO)
Jones, Sally	Licensing Agent
Thomas, Jack	IT Manager

If you have any questions, you can reach me at (800) 555-5555 Ext 1.

Sincerely,

Sandy Anderson  
Local Agency Security Officer  
Licensing Manager, ZYX Gaming Commission

Updated 2/24/2020

# Appendix J

## SAMPLE NONCRIMINAL JUSTICE AGENCY TRAINING DOCUMENTATION FORM

AGENCY NAME: \_\_\_\_\_ OCA: \_\_\_\_\_

**The following training is REQUIRED:**

Security Awareness Training (CJIS Online)

This training must be completed within 6 months of hire or appointment to position with access to criminal justice/criminal history record information. It must be repeated every two years for as long as the individual is on the agency Authorized Personnel List and granted access to criminal justice and/or criminal history record information.

Agency Internal Privacy and Security Training

Any personnel placed on the agency authorized Personnel List should receive internal agency training on the agency's security and handling processes prior to being allowed access to criminal justice and/or criminal history record information. Refresher training shall be completed every two years.

Name	First Time (F) or Refresher Training (R)?	Date of Security Awareness Training (CJIS online)	Date of Agency Privacy & Security Training	Acknowledgement Statement Signed? (Y/N)
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				

The persons named above have received the required training in accordance with applicable rules and regulations.

LASO Printed Name: \_\_\_\_\_ LASO Signature: \_\_\_\_\_ Date: \_\_\_\_\_

PLEASE PRINT LEGIBLY- Keep training logs on file. Training logs will be reviewed during audits. The National Indian Gaming Commission (NIGC) will also periodically request the agency submit training logs as part of quality assurance and compliance review. Please do not send training logs to the NIGC unless requested.

## Appendix K

### National Indian Gaming Commission Fingerprint MOU/CJIS Checklist

Tribe/TGRA:	Date:
NIGC Compliance Officer:	LASO:
<b>Authority</b>	
Under what authority does the TGRA access CHRI?	IGRA _____ State Statute _____ If yes, name/citation: _____ Other _____
<b>Purpose</b>	
Does the TGRA have an executed Memorandum of Understanding with the NIGC dated 2017 or later?	Yes _____ No _____
Have all Authorized Personnel who access CHRI received and reviewed the MOU?	Yes _____ No _____
Does your TGRA audit or review to ensure only fingerprint are submitted for employees of the gaming operation who are classified as Key Employees or Primary Management Officials as defined in 25 C.F.R. 502.14 (a-c) or 502.19 (a-c)? (Policy Required)	Yes _____ Method of verification _____ No _____
How does the TGRA background applicants who are classified as Key Employees or Primary Management Officials as defined in 25 C.F.R. 502.14 (d) or 502.19 (d)? (Policy Required)	Method Used _____  Approved gaming ordinance page, where the definitions of these PMOs and KEs are located: _____
Are there applicant positions that are no longer fingerprinted through the NIGC after the review?	Yes _____ List Positions _____ No _____
Are there applicant positions that require additional TGRA review or consideration by the NIGC?	Yes _____ List Positions _____ No _____
Are there applicant positions that are not classified as Key Employees or Primary Management Officials as defined in 25 C.F.R.	Yes _____ Provide Justification _____ No _____

502.14 (a-c) or 502.19 (a-c) which are still being fingerprinted?	
<b>Fingerprint Submissions</b>	
Are fingerprints processed through NIGC? *If yes, continue review. If no, completion of checklist is voluntary.	Yes _____ No _____
What methods are used to capture and submit fingerprints?	Hard Card Submission? _____ Electronic Submission? _____
Prior to fingerprinting the applicant, does the TGRA verify the identity of the individual being fingerprinted? (Policy Required)	Yes _____ By what means? _____ No _____
Prior to submitting fingerprints, does the TGRA notify the individual fingerprinted in writing <sup>3</sup> that the fingerprints will be used to check the Criminal History Records of the FBI (28 C.F.R. 50.12(b))?	Yes _____ No _____
Prior to submitting the fingerprints, does the TGRA ensure the applicant receives the FBI Privacy Act notice that is dated 2013 or later? (Policy Required)	Yes _____ No _____
Prior to submitting fingerprints, does the TGRA ensure the applicant receives the FBI Noncriminal Justice Applicants Rights Notice? (Policy Required)	Yes _____ No _____
Does the TGRA complete the Reason for Fingerprint (RFP) field to ensure the correct RFP is used? (INDIAN GAMING LICENSEE)	Yes _____ No _____
Does the TGRA submit fingerprints for other agencies? (Strictly Prohibited)	Yes _____ Which ones? _____ No _____
<b>Receipt of Criminal History Record Information (CHRI)</b>	
Does the TGRA receive CHRI results after the submission of a fingerprint-based transaction?	Yes _____ No _____
How does the TGRA receive the CHRI?	Mail (hard copy) _____ Email _____ Live Scan Device _____
<b>Use of Criminal History Record Information (CHRI)</b>	
For what purpose does the TGRA use the CHRI? (Policy Required)	Licensing _____ Employment _____ Other _____ Please describe: _____

<sup>3</sup> Written notification includes electronic notification but excludes oral notification.

What other TGRA documents/situations contain CHRI or summary CHRI?	Notice of Results _____ Investigative Reports _____ Objection Letters _____ Spreadsheets _____	Phone Calls _____ Databases _____ Meeting Notes _____ Other _____
Is CHRI or summary CHRI reused for any other purpose after the initial inquiry?	Yes _____ No _____ If yes, Explain: _____	
Who has access to the CHRI? (Policy Required, Outsourcing Agreements may be required)	Licensing Staff _____ Other Department(s) (e.g., IT) _____ Other Agency Contractor(s) _____ Other _____	
Is CHRI or summary CHRI disseminated to or shared with any entity other than the NIGC?	Yes _____ No _____ If yes, explain who, when, and under what circumstances: _____	
<b>Applicant Involvement</b>		
Does the TGRA provide the applicant an opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record (28 C.F.R. 50.12 (b))? (Policy Required)	Yes _____ No _____	
If Yes to the above question, does the TGRA advise the applicant in writing <sup>4</sup> of the procedures for obtaining a change, correction, or update of an FBI identification record, as set forth in 28 C.F.R. 16.34 (DO Process)? (28 C.F.R. 50.12 (b)) (Policy Required)	Yes _____ If yes, describe how: _____  No _____	
Does the TGRA provide the applicant reasonable time to correct or complete the record (or decline to do so) before the TGRA takes action on their license or employment? (Policy Required)	Yes _____ How much time is provided? _____ No _____	
Does the TGRA choose to disseminate the applicant's CHRI record to the applicant? (Policy Required)	Yes _____ No _____	
If Yes to the above question, does the TGRA verify the applicant's identity prior to	Yes _____ How? _____ No _____	

<sup>4</sup> Written notification includes electronic notification but excludes oral notification.

disseminating a copy to the applicant or their attorney working on their behalf?	
If Yes to the above question, does the TGRA document the release and mark the CHRI in a way to determine the document is a copy?	Yes _____ How? _____ No _____
If No to the above question, does the TGRA advise the applicants how to obtain the CHRI record from the FBI directly? (Policy Required)	Yes _____ No _____
<b>Handling of Criminal History Record Information (CHRI)</b>	
Does the TGRA have a retention policy/procedure for CHRI? (Policy Required)	Yes _____ No _____
Does the TGRA retain CHRI (hard copies or electronic), or documents containing CHRI or summaries of it? (Policy Required)	Yes _____ No _____
If the TGRA does retain CHRI, how long are they stored? (Policy Required)	Time _____
When retention of CHRI is no longer required, what is the method of disposal? (Policy Required)	Shred _____ Incinerate _____ Routine Trash _____ Overwriting 3 or more times _____ Degaussing _____ Other _____
Do Authorized Personnel complete the disposal of CHRI? (Policy Required)	Yes _____ No _____
If No to the above question, do Authorized Personnel oversee the CHRI destruction? (Policy Required)	Yes _____ No _____
<b>Local Agency Security Officer Responsibilities</b>	
Has the TGRA designated a Local Agency Security Officer (LASO)? (Policy Required)	Yes _____ No _____
Does the LASO update the Tribal and TGRA information with the NIGC if changes occur? (Policy Required)	Yes _____ No _____
Has the LASO submitted the Authorized Personnel List to the NIGC and submits updated lists as needed? (Policy Required)	Yes _____ No _____
Have all Authorized Personnel signed the Tribe's Acknowledgement Statement? (Policy Required)	Yes _____ No _____
Has the LASO completed training required	Yes _____ Through what means? _____

under CJIS Policy 5.2.2 prior to assuming the LASO duties and annually thereafter? (Policy Required)	No _____
Has the LASO ensured all Authorized Personnel have received FBI Security Awareness Training within 6 months of being placed on the Authorized Personnel List or their date of hire and every two years thereafter? (Policy Required)	Yes _____ Through what means? _____ No _____
Has the LASO ensured the Tribe has adequate policies and procedures related to access, use, handling, dissemination and destruction of CJI/CHRI? (Policies Required)	Yes _____ Please list the name of each: _____ No _____
Has the LASO ensured all Authorized Personnel have received internal training on approved policies and procedures regarding CHRI within 6 months of being placed on the Authorized Personnel List or their date of hire and every two years thereafter? (Policy Required)	Yes _____ No _____
Has the LASO implemented a security incident reporting policy which requires notification of findings be reported to the NIGC within 24 hours of detection? (Policy Required)	Yes _____ No _____
Does the LASO complete a training documentation form for the above trainings and retain the document for audit purposes? Are Security Awareness Training records maintained for a minimum of two years? (Policy Required)	Yes _____ No _____
Does the LASO audit to ensure each fingerprint submission is for the specific purpose of Key Employee and Primary Management official employments and is made pursuant to the authority to access the CHRI? (Policy Required)	Yes _____ No _____
<b>Outsourcing Agreements</b>	
Does the TGRA have an FBI Compact Council approved outsourcing agreements <sup>5</sup> for all entities with access to CHRI? (Policy Required)	Yes _____ No _____
Does the TGRA audit the entity's compliance	Yes _____

<sup>5</sup> Such approval must be in writing and provided prior to the contracts being entered into or the entity accessing CJI or CHRI.

with the CJIS Security Policy within 90 days of entering the outsourcing agreement? (Policy Required)	No _____
<b>Resource Documents</b>	
Indian Gaming Regulatory Act	<a href="https://www.govinfo.gov/content/pkg/USCODE-2014-title25/pdf/USCODE-2014-title25-chap29.pdf">https://www.govinfo.gov/content/pkg/USCODE-2014-title25/pdf/USCODE-2014-title25-chap29.pdf</a>
FBI CJIS Security Policy	<a href="https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center">https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center</a>
Noncriminal Justice IT Security Audit	<a href="https://www.nigc.gov/compliance/CJIS-Training-Materials">https://www.nigc.gov/compliance/CJIS-Training-Materials</a>
FBI Security Awareness Training PowerPoint Presentation	<a href="https://www.nigc.gov/compliance/CJIS-Training-Materials">https://www.nigc.gov/compliance/CJIS-Training-Materials</a>
Draft Information Technology Security Policy Templates	<a href="https://www.fbi.gov/services/cjis/compact-council/sanctions-process-information">https://www.fbi.gov/services/cjis/compact-council/sanctions-process-information</a>
FBI Privacy Act Statement	<a href="https://www.fbi.gov/services/cjis/compact-council/privacy-act-statement">https://www.fbi.gov/services/cjis/compact-council/privacy-act-statement</a>
Noncriminal Justice Applicant's Privacy Rights Notice	<a href="https://www.fbi.gov/services/cjis/compact-council/guiding-principles-noncriminal-justice-applicants-privacy-rights">https://www.fbi.gov/services/cjis/compact-council/guiding-principles-noncriminal-justice-applicants-privacy-rights</a>
Outsourcing of Noncriminal Justice Functions Guide	<a href="https://www.nigc.gov/compliance/CJIS-Training-Materials">https://www.nigc.gov/compliance/CJIS-Training-Materials</a>
<b>CJIS Contact Information</b>	
Mr. Virgilio Congmon NIGC Information Security Officer iso@nigc.gov (202) 632-7003	Mr. Shea Bennett NIGC CJIS Systems Officer itsupport@ngic.gov (202) 632- 7003
Chasity S. Anderson FBI Compact Officer FBI / CJIS Division csanderson@fbi.gov (304) 625-2803 (office) (304) 476-3383 (mobile)	John C. Weatherly FBI CJIS ISO FBI/CJIS jcweatherly@fbi.gov (304) 625-3660 (office) (304) 709-1493 (mobile)

Updated 2/24/2020

**Noncriminal Justice Agency  
(NCJA)  
Information Technology  
Security Audit  
Correspondence Questionnaire**



**Agency Contact Information**

Please complete the following, where applicable only.

**Audit Information:**

Agency Name/Department Name: \_\_\_\_\_  
ORI/Unique Identifier: \_\_\_\_\_  
Name of Agency Head: \_\_\_\_\_ Title: \_\_\_\_\_  
Mailing Address: \_\_\_\_\_

**Primary Point of Contact (POC):**

Name: \_\_\_\_\_ Title: \_\_\_\_\_  
Street Address: \_\_\_\_\_ City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
Phone: \_\_\_\_\_ Alt. Phone: \_\_\_\_\_ Email: \_\_\_\_\_

**Local Agency Security Officer (LASO) (technical POC, if applicable):**

Name: \_\_\_\_\_ Title: \_\_\_\_\_  
Street Address: \_\_\_\_\_ City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
Phone: \_\_\_\_\_ Alt. Phone: \_\_\_\_\_ Email: \_\_\_\_\_

**Physical Address (main address where CHRI/CJI is accessed):**

Contact Name: \_\_\_\_\_ Title: \_\_\_\_\_  
Street Address: \_\_\_\_\_ City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
Phone: \_\_\_\_\_ Alt. Phone: \_\_\_\_\_ Email: \_\_\_\_\_

**Data Center (if different from physical address):**

Contact Name: \_\_\_\_\_ Title: \_\_\_\_\_  
Street Address: \_\_\_\_\_ City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
Phone: \_\_\_\_\_ Alt. Phone: \_\_\_\_\_ Email: \_\_\_\_\_

**Offsite Media Storage (where media containing CJI is stored outside of the agency):**

Contact Name: \_\_\_\_\_ Title: \_\_\_\_\_  
Street Address: \_\_\_\_\_ City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
Phone: \_\_\_\_\_ Alt. Phone: \_\_\_\_\_ Email: \_\_\_\_\_

**Back-up Recovery Site (disaster recovery site/where system back-ups are stored):**

Contact Name: \_\_\_\_\_ Title: \_\_\_\_\_  
Street Address: \_\_\_\_\_ City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
Phone: \_\_\_\_\_ Alt. Phone: \_\_\_\_\_ Email: \_\_\_\_\_

**AUTHORIZED USE/ACCESS TO CRIMINAL JUSTICE INFORMATION**

**\*\*\*Please note criminal history record information (CHRI) is a subset of criminal justice information (CJI) and are interchangeable for the purposes of this document.\*\*\***

1. Under what authority does the agency have access to national CHRI/CJI?

- State statute: \_\_\_\_\_
- NCPA/VCA
- Adam Walsh Act
- HUD (Housing and Urban Development) / PHA (Public Housing Authority)
- Real ID Act
- Other: \_\_\_\_\_

2. Does the agency have access to CHRI/CJI by means other than fingerprint submission?

- YES  NO  N/A

3. Describe the process for the submission of civil fingerprint transactions to include method of submission to the state Repository.

---

---

---

---

---

4. How does the agency receive or retrieve the national CHRI response from the state Repository?

- mail (hard copy)
- fax
- email
- website
- livescan device
- other: \_\_\_\_\_

**RETENTION OF CRIMINAL JUSTICE INFORMATION**

1. Does the agency retain the results (hard copies or electronic) of the criminal history record check or documents containing CHRI/CJI?  YES  NO  N/A

- hard copy (case files, filing cabinet, etc.)
- e-mail (kept on email server/archive)
- scanned/saved to network share (more than one person can access)
- Excel spreadsheet (yes/no indicators kept, etc.)
- scanned/saved to desktop (not on network file share)
- website/internet application (records management system/personnel database, etc.)
- other: \_\_\_\_\_

2. Is the CHRI/CJI commingled (kept in same location) with any other records (such as in a personnel file with tax information, etc.)?  YES  NO  N/A

**DISSEMINATION OF CRIMINAL JUSTICE INFORMATION**

1. Does the agency disseminate CHRI/CJI results to the individual of record or applicant?  YES  NO  N/A

a. How is the information disseminated?

- mail (hard copy)
- courier service
- hand carried by authorized personnel
- email
- website/internet
- verbal (face to face or by phone)
- fax
- other: \_\_\_\_\_

2. Does the agency disseminate CHRI/CJI to any other entity/individual?  YES  NO  N/A

a. Who?

- private contractors (for outsourcing – additional questions below)
- another similar agency (e.g. one school to another school)
- grant funded positions (give results to grant provider)
- accreditations (providing CHRI to accreditation company for review/proof)
- licensing
- audit (other than FBI/State Repository)
- other: \_\_\_\_\_
- other: \_\_\_\_\_

b. How is the CHRI/CJI shared?

- mail (hard copy)
- courier service
- hand carried by authorized personnel
- email
- website/internet
- Verbal (face to face or by phone)
- fax
- other: \_\_\_\_\_

c. What information is sent?

\_\_\_\_\_  
\_\_\_\_\_

d. Why is the information sent/for what purposes would you disclose the results?

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

3. How is the information protected during dissemination?

- encryption (if via email, accessed via an internet website or application)
- tamper-proof container (sealed envelope, locked container, etc.)
- hand carried by authorized personnel
- certified mail
- other: \_\_\_\_\_

a. If CHRI/CJI is sent via email or accessed from an internet based application or website, please describe methods (bit level such as 128, hardware/software, etc.) of encryption and the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 140-2 certification number.

\_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_

b. Does the agency protect the information using a passphrase (to unlock encryption)? Please describe.

\_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_

**ADMINISTRATION OF NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS**

**PRIVATE CONTRACTORS**

1. Does the agency outsource (use private contractor personnel/vendors) for any noncriminal justice administrative functions that provides private contractor personnel with access to CHRI/CJI?

YES  NO  N/A

a. If YES, what noncriminal justice administrative functions are private contractors performing?

- data destruction (paper shredding, hard drives, etc.)
- IT services (network/system administrations, desktop support, etc.)
- off-site media storage (data centers, backup, paper storage archives, etc.)
- dispositions (obtains additional information from court of jurisdiction)
- hiring decisions (mails offer letters, generates security badges/credentials, etc.)
- scanning services (scans results into database or electronic file)
- other: \_\_\_\_\_

b. Has the agency obtained state/repository level approval for private contractor access to CHRI/CJI?

YES  NO  N/A

c. Has the agency designated someone as an Agency Coordinator to ensure all private contractor personnel have completed a fingerprint based record check (if applicable), completed the appropriate level security awareness training, and abide by all policies within the CJIS Security Policy?

YES  NO  N/A

- d. Does the agency have a contract/agreement with the private contractor(s), which incorporates or references the CJIS Security Policy and Outsourcing Standard?  YES  NO  N/A

PERSONNEL SECURITY

1. Has the state passed legislation authorizing or requesting civil fingerprint-based record checks for personnel with access to CHRI/CJI for the purposes other than the administration of criminal justice functions (*e.g., licensing and employment*)?  YES  NO  N/A
- a. If **YES**, has the agency ensured all personnel with unescorted access to CHRI/CJI have completed a state and national fingerprint-based record check within 30 days of access to CHRI/CJI? (*should include agency personnel, IT staff, private contractors, cleaning/maintenance personnel with physical access to secure locations*)  YES  NO  N/A

SECURITY AWARENESS TRAINING

1. Does the agency ensure all personnel with unescorted access to CHRI/CJI have completed security awareness training within 6 months of assignments and at least every two years after? (*should include agency personnel, IT staff, private contractors, cleaning/maintenance personnel with physical access to information*)  YES  NO  N/A
- a. If **YES**, is documentation of individual security awareness training maintained in a current status, to include private contractors if applicable?  YES  NO  N/A
- b. Is the agency using the state provided training curriculum? (If **NO**, please provide training materials for review)
- YES  NO  N/A

SECURITY INCIDENTS AND VIOLATIONS

1. Does the agency provide and enforce the CJIS Security Policy to all authorized users, to include private contractor personnel?  YES  NO  N/A
2. Does the agency have a written policy for the discipline of CJIS policy violators?  YES  NO  N/A
3. What are the procedures when a security violation or incident is detected?
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- a. Does the agency report the security violation or incident to anyone? Who?  YES  NO  N/A
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- b. Are all employees and/or private contractors made aware of the reporting procedures?  YES  NO  N/A

- c. Are the procedures described above written in agency policy?  YES  NO  N/A
4. Has the agency reported/had any security violations or incidents in the last 3 years? (incidents in which security of CHRI/CJI was compromised or put at risk)  YES  NO  N/A

---



---



---



---

### INFORMATION PROTECTION

**\*\*\*Please note, if the agency does not retain criminal history record information or criminal justice information, the following sections are not applicable. Please skip each section that is not applicable and complete the signature block on the last page of this questionnaire before returning as indicated.\*\*\***

#### FOR HARD COPY STORAGE AND ACCESSIBILITY

**The following questions apply to noncriminal justice agencies retaining all or part of the national criminal history record in paper (hard copy) form.**

1. Describe all locations where and how criminal history record information is retained. (e.g. locked file cabinet, locked office, off-site storage facility, records archive, etc.)
   

---



---



---



---
  
2. Is the storage location physically secured? (i.e. unauthorized personnel cannot access CHRI/CJI, within a locked file with limited access, in a locked office, in a safe, etc.)  YES  NO  N/A
  - a. Does the agency house files that contain CHRI/CJI in an off-site record storage facility?  YES  NO  N/A
  - b. Who owns/manages the facility? (i.e. who controls access)
   

---
  - c. How are records transported to the off-site facility?
   

---
  - d. How are the records stored at the off-site facility?
   

---
  
3. Does the agency have a written policy that describes physical protections? (i.e. how and where the information must be stored, who can access, restricts unauthorized access, requires visitors to be escorted, etc.)  YES  NO  N/A
4. Are visitors escorted by authorized personnel in physically secure locations at all times (in all access and storage areas to include off-site facilities if designated physically secure)?  YES  NO  N/A

5. How does the agency dispose of physical (hard copy/paper) media containing CHRI/CJI?

---

---

---

---

- a. Does the agency have written procedures for paper destruction?  YES  NO  N/A
- b. If the agency personnel does not conduct the sanitization or destruction of the media and it is performed by another entity, is the process witnessed by authorized personnel?  
 YES  NO  N/A

FOR SINGLE DESKTOP STORAGE AND ACCESSIBILITY

**The following questions apply to noncriminal justice agencies retaining all or part of the criminal history record on a single computer (desktop, laptop, tablet, etc.) that is not part of a larger shared network. (i.e. one user/one desktop)**

1. What information is kept? (i.e. scanned copies, excel spreadsheet with CHRI/CJI indicators, word documents with descriptors, email account, etc.)

---

---

---

---

2. Describe the physical location where the computer with access to CHRI/CJI is housed. (e.g., locked office, reception area, etc.)

---

---

---

---

a. Is the computer's location physically secured? (i.e. unauthorized personnel cannot access CHRI/CJI, computer is not left unattended, visitors are escorted while in area, etc.)  YES  NO  N/A

b. Is the CHRI/CJI encrypted at rest?  YES  NO  N/A

c. If encryption is used, please describe methods (bit level, hardware/software, etc.) of encryption. (e.g. Adobe Pro, WinZip, TrueCrypt, etc.)

---

---

---

d. Does the agency protect the information using a passphrase (to unlock encryption)? Please describe.

---

---

---

3. Does the agency have a written policy that describes physical protections? (i.e. how and where the information/equipment must be stored, who can access, restricts unauthorized access, requires visitors to be escorted, etc.)  YES  NO  N/A

4. When a computer reaches end of life (no longer works) or is to be replaced/upgraded, how does the agency destroy the hard drive?

---

---

---

---

a. Does the agency have written procedures for the sanitization and/or destruction of electronic media (hard drive, thumb drive, CDs, etc.)?  YES  NO  N/A

b. If the agency personnel does not conduct the sanitization or destruction of the media and it is performed by another entity, is the process witnessed by authorized personnel?  
 YES  NO  N/A

5. When logging onto the computer or before accessing CHRI/CJI does the user enter a password that utilizes secure password attributes? (at least 8 characters, numbers/letters, expires every 90 days, cannot reuse 10 previous passwords, and does not display when entered)  YES  NO  N/A

6. Do users ever share their usernames, password, or passphrase (if applicable)?  YES  NO  N/A

7. Does the computer initiate a session lock (require the user to re-enter password) after a maximum of 30 minutes of inactivity?  YES  NO  N/A

a. If a user leaves the computer, do they log out of the computer or lock the screen?  
 YES  NO  N/A

8. Does the agency apply routine patches and updates to all software and components? (i.e. Windows updates, virus protection patches, etc.)  YES  NO  N/A

9. Does the computer storing CHRI/CJI have access to the internet?  YES  NO  N/A

a. If **YES**, describe the boundary protection used to protect the computer. (i.e., hardware/software firewalls, proxies, gateways, guards, routers, etc.)

---

---

b. Does the agency enable virus protection at start-up and employ automatic scanning and updates?  
Please describe.  YES  NO  N/A

---

10. Does someone within the agency stay up to date with relevant security alerts and advisories?  YES  NO  N/A

FOR SHARED NETWORK STORAGE AND ACCESSIBILITY

**The following questions apply to noncriminal justice agencies retaining all or part of the criminal history record on a shared closed-network platform (not accessible from internet webpage).**

1. What information is kept? (i.e. scanned copies, excel spreadsheet with CHRI/CJI indicators, word documents with descriptors, emails, etc.)

---

---

---

---

2. Identify all locations where CHRI/CJI is either maintained (stored) or can be accessed (e.g., servers, offsite backups, primary offices, secondary locations, third party cloud storage, etc.)

---

---

---

---

- a. Are all locations where CHRI/CJI is either maintained/stored or accessed considered physically secured? (i.e. unauthorized personnel cannot access CHRI/CJI, computer is not left unattended, visitors are escorted while in area, etc.)  YES  NO  N/A

- b. Describe physical security measures. (i.e. key card access, locked doors, etc.)

---

---

---

- c. Is the CHRI/CJI encrypted at rest?  YES  NO  N/A

- d. Is the CHRI/CJI encrypted in transit? (accessed from secondary location, emailed, remotely accessed)  YES  NO  N/A

- e. If encryption is used, please describe methods (bit level, hardware/software, etc.) of encryption. (e.g. Adobe Pro, WinZip, TrueCrypt, etc.)

---

---

---

- f. Does the agency protect the information using a passphrase (to unlock encryption)?

Please describe.

YES  NO  N/A

---

---

---

3. Does the agency have a written policy that describes physical protections? (i.e. how and where the information/equipment must be stored, who can access, restricts unauthorized access, requires visitors to be escorted, etc.)  YES  NO  N/A

4. Is the CHRI/CJI backed up to off-site storage or a disaster recovery location?  YES  NO  N/A

a. Who owns/manages the facility? (i.e. who controls access)

\_\_\_\_\_

b. How are backup records transported to the secondary facility? (i.e. disc to disc with encryption or physical tapes encrypted or in locked box, etc.)

\_\_\_\_\_

c. How are the records stored at the off-site facility?

\_\_\_\_\_

5. When a computer reaches end of life (no longer works) or is to be replaced/upgraded, how does the agency destroy the hard drive?

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

a. Does the agency have written procedures for the sanitization and/or destruction of electronic media (hard drive, thumb drive, CDs, etc.)?  YES  NO  N/A

b. If the agency personnel does not conduct the sanitization or destruction of the media and it is performed by another entity, is the process witnessed by authorized personnel?  
 YES  NO  N/A

6. Before logging into the computer or before accessing CHRI/CJI, does the agency display a system use notification, a warning to the user that they are accessing sensitive information and informing of the possible consequences for misuse?  YES  NO  N/A

7. When logging onto the computer or before accessing CHRI/CJI does the user enter a password that utilizes secure password attributes? (at least 8 characters, numbers/letters, expires every 90 days, cannot reuse 10 previous passwords, and does not display when entered)  YES  NO  N/A

8. Do users ever share their usernames, passwords, or passphrase (if applicable)?  YES  NO  N/A

9. Describe the agency's process for issuing user accounts, deleting/disabling user accounts, and periodic validation of user accounts:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

a. Are these procedures written?  YES  NO  N/A

10. Does the information system initiate a session lock (require the user to re-enter password) after a maximum of 30 minutes of inactivity?  YES  NO  N/A

a. If a user leaves the computer, do they log out of the computer or lock the screen?  
 YES  NO  N/A

11. Does the information system log:  YES  NO  N/A

- successful and unsuccessful log on attempts
- successful and unsuccessful password changes
- successful and unsuccessful actions by privileged accounts (adding users, deleting users, etc.)
- successful and unsuccessful actions related to CHRI (delete records, edits of information, access to the record, etc.)

a. Does each logged event include: date, time, component (where it occurred), type of event, user, outcome (success or failure)?  YES  NO  N/A

b. Does the agency check logs (who accessed CHRI/CJI, logged in, etc.) at least weekly?  
 YES  NO  N/A

c. How long are logs kept?  
\_\_\_\_\_

12. Does the agency apply routine patches and updates to all software and components? (i.e. Windows updates, firewall patches, etc.)  YES  NO  N/A

13. Describe the boundary protection used to protect the network. (i.e., hardware/software firewalls, proxies, gateways, guards, routers, etc.)  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

a. Is CHRI/CJI separated from non-CHRI/CJI related access? (i.e. can unauthorized users access shared folder or location of CHRI/CJI or is it separated in some way, such as a VLAN?)

Please describe.  YES  NO  N/A  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

14. Does the agency utilize intrusion detection (IDS) or intrusion protection (IPS) tools?  
 YES  NO  N/A  
\_\_\_\_\_

15. Can users access CHRI/CJI remotely? (i.e., access network from outside physically secure location, etc.) Please describe. (i.e. method/application, encryption used, etc.) Include details. (e.g., Citrix, VPN, GoToMyPC, LogMeIn, TeamViewer, etc.)  YES  NO  N/A  
\_\_\_\_\_  
\_\_\_\_\_

16. Does the agency enable virus protection at start-up and employ automatic scanning and updates on all computers and servers storing or accessing CHRI/CJI? Please describe. (i.e. type and version)  
 YES  NO  N/A

---

17. Does someone within the agency stay up to date with relevant security alerts and advisories?  YES  NO  N/A

18. Does the agency host any CHRI/CJI in a virtualized environment?  YES  NO  N/A

a. Please describe how CHRI information is protected in a virtual environment. (i.e. how is CHRI protected from unauthorized access – partitions, separate virtual NICs, different hosts from non-CHRI related systems or internet facing applications, etc.?)

---

---

---

---

**FOR RECORD MANAGEMENT SYSTEMS/DATABASE STORAGE AND INTERNET ACCESSABILITY**

**The following questions apply to noncriminal justice agencies retaining all or part of the criminal history record in a records management system or database that is accessible through the internet.**

1. What information is kept? (i.e. scanned copies, entered descriptor data, etc.)

---

---

---

---

2. What is the name of the application/website/database housing CHRI/CJI? (i.e. HR database, etc.)

---

3. Identify all locations where criminal history information/CJI is maintained/stored. (e.g., application/web servers, database storage, offsite backups, primary offices, secondary locations, third party cloud storage, etc.)

---

---

---

---

a. Are all locations where CHRI is either maintained/stored considered physically secured? (i.e. unauthorized personnel cannot access CHRI, computer is not left unattended, visitors are escorted while in area, etc.)  YES  NO  N/A

b. Describe physical security measures. (i.e. key card access, locked doors, etc.)

---

---

c. Is the CHRI or CJI encrypted at rest?  YES  NO  N/A

d. If encryption is used for data at rest, please describe methods (bit level, hardware/software, etc.) of encryption.

---

---

---

4. Does the agency have a written policy that describes physical protections? (i.e. how and where the information/equipment must be stored, who can access, restricts unauthorized access, requires visitors to be escorted, etc.)  YES  NO  N/A

5. Is the CHRI/CJI backed up to off-site storage or a disaster recovery location?  YES  NO  N/A

a. Who owns/manages the facility? (i.e. who controls access)

---

b. How are backup records transported to the secondary facility? (i.e. disc to disc with encryption or physical tapes encrypted or in locked box, etc.)

---

c. How are the records stored at the off-site facility?

---

6. When a computer/server, etc. reaches end of life (no longer works) or is to be replaced/upgraded, how does the agency destroy the hard drive?

---

---

---

---

a. Does the agency have written procedures for the sanitization and/or destruction of electronic media (hard drive, thumb drive, CDs, etc.)?

YES  NO  N/A

b. If the agency personnel does not conduct the sanitization or destruction of the media and it is performed by another entity, is the process witnessed by authorized personnel?

YES  NO  N/A

7. Before logging into the application or website to access CHRI/CJI, does the agency display a system use notification, a warning to the user that they are accessing sensitive information and informing of the possible consequences for misuse?  YES  NO  N/A

8. When logging onto the application or website and accessing CHRI/CJI does the user and/or administrator enter a password that utilizes secure password attributes that includes all of the following characteristics?  YES  NO  N/A

- length must be at least eight characters
- must contain letters and numbers or special characters
- not be the same as the user ID
- expire within a maximum of 90 days
- not allow the reuse of the last 10 passwords
- not display when entered

9. Do users or IT administrators ever share their usernames or passwords or have generic group accounts?  YES  NO  N/A

10. Describe the agency's process for issuing user accounts, deleting/disabling user accounts, and periodic validation of user accounts:

---

---

---

---

a. Are these procedures written?  YES  NO  N/A

11. Does the information system or application initiate a session lock (require the user to re-enter password) after a maximum of 30 minutes of inactivity?  YES  NO  N/A

a. If a user leaves the computer, do they log out of the computer or lock the screen?  YES  NO  N/A

12. Are the following events logged:  YES  NO  N/A

- successful and unsuccessful log on attempts
- successful and unsuccessful password changes
- successful and unsuccessful actions by privileged accounts (adding users, deleting users, etc.)
- successful and unsuccessful actions related to CHRI (delete records, edits of information, access to the record, etc.)

a. Does each logged event include: date, time, component (where it occurred), type of event, user, outcome (success or failure)?  YES  NO  N/A

b. If a security incident happened in relation to the release or misuse of CHRI/CJI, could you identify the individual who carried out the action and when?  YES  NO  N/A

c. Does the agency check logs (who accessed CHRI/CJI, logged in, etc.) at least weekly?  YES  NO  N/A

d. How long are logs kept?

---

13. Does the agency apply routine patches and updates to all software and components? (i.e. Windows updates, firewall patches, etc.)  YES  NO  N/A

14. Describe the boundary protection used to protect the network. (i.e., hardware/software firewalls, proxies, gateways, guards, routers, etc.)

---

---

---

---

a. Is CHRI/CJI separated from non-CHRI/CJI related access? (i.e. can unauthorized users access application or locations of CHRI/CJI or is it separated in some way, such as a VLAN?)

Please describe.  YES  NO  N/A

---

---

---

15. Does the agency utilize intrusion detection (IDS) or intrusion protection (IPS) tools?

YES  NO  N/A

---

16. How is CHRI/CJI encrypted when transmitted outside the physically secure location where it is stored? (i.e., how is the data encrypted when a user is accessing from an internet connection, etc.) Include details. (e.g., methods of encryption, bit level, hardware/software/application, FIPS certificate numbers, etc.)

---

---

---

---

17. Does the agency enable virus protection at start-up and employ automatic scanning and updates on all computers and servers storing or accessing CHRI/CJI? Please describe. (i.e. type and version)

YES  NO  N/A

---

18. Does someone within the agency stay up to date with relevant security alerts and advisories?

YES  NO  N/A

19. Does the agency host any CHRI/CJI in a virtualized environment?

YES  NO  N/A

a. Please describe how CHRI information is protected in a virtual environment. (i.e. how is CHRI protected from unauthorized access – partitions, separate virtual NICs, different hosts from non-CHRI related systems or internet facing applications, etc.)

---

---

---

---

**Before returning this audit, please complete the following information:**

Questionnaire Completed By (signed name): \_\_\_\_\_

Questionnaire Completed By (print name): \_\_\_\_\_

Phone Number: \_\_\_\_\_ Date Completed: \_\_\_\_\_

E-mail address: \_\_\_\_\_

**After completed, please attach all supporting documentation and send to the following:**

Attention: \_\_\_\_\_

Phone: \_\_\_\_\_ Fax: \_\_\_\_\_

Email: \_\_\_\_\_

Mailing Address: Street: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_

**\*\*\*\*\* FOR OFFICIAL USE ONLY\*\*\*\*\***

**Auditor Review**

Auditor Name: \_\_\_\_\_ Date of Review: \_\_\_\_\_

Comments/Documents Provided/Notes: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Secondary Reviewer: \_\_\_\_\_ Date of Review: \_\_\_\_\_

Additional Comments: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

## Appendix L

### **Key Employee/ Primary Management Official Classification Guide for CHRI MOU Compliance**

Under the 2020 Memorandum of Understanding (MOU) with the FBI, the National Indian Gaming Commission (NIGC) agrees to use CHRI solely for the purpose of determining an applicant's eligibility for employment as a key employee or primary management official at the Tribe's gaming operation, as defined in NIGC regulations, **25 C.F.R. §§ 502.14(a) – (c) and 502.19(a) – (c)**, and not for any other purpose.<sup>6</sup>

If a Tribe has an executed MOU with the NIGC, Tribes are permitted to submit fingerprints to the FBI through the NIGC to obtain and use Criminal History Record Information (CHRI) for the sole purpose of making an employment and/or licensing determination of KEs and PMOs as defined in the FBI/NIGC MOU. The NIGC offers the following technical assistance to tribal gaming regulatory authorities (TGRAs) for determining whether an applicant meets the definitions in the FBI/NIGC MOU.

Though there are some limitations, the position title can be an important indicator as to whether or not a gaming operation employee is a KE or a PMO. The proper classification of a gaming operation employee, however, depends upon the specific duties and responsibilities of the individual in their job/position. For example, a Food and Beverage Manager, as an employee of a gaming operation with an annual compensation of \$47,000, without the ability to hire or fire employees, who does not handle cash or gaming supplies, is not a KE. But if the same Food and Beverage Manager gets a raise and makes in excess of \$50,000 in a year, becomes a KE. Another example is Environmental Services (EVS) staff. In general, EVS staff are employees of a gaming operation with individual "total cash compensation" less than \$50,000 a year. Nevertheless, if when the TGRA examines the individual's specific duties and determines that the night-shift EVS employee performs additional duties normally completed by a KE, the EVS employee is a KE. These duties must include one or more listed in NIGC regulation, 25 C.F.R. § 502.14 (a)-(c), such as accessing or handling gaming equipment, gaming revenue, or gaming revenue accounting records (including revenue records in gaming equipment). Once an employee's position transforms into a KE position, the employee must go through the KE licensing process and their fingerprints may be submitted through NIGC for purposes of receiving their criminal history record.

To ensure CHRI MOU compliance, Tribes with an executed MOU are required to determine whether applicants meet the FBI/MOU definitions of a KE or a PMO prior to submitting fingerprints through the NIGC. The following questions should help guide the TGRA to properly classify such applicants. If additional analysis or further guidance is needed, please contact NIGC region staff.

#### Questions for KE Classification

---

<sup>6</sup> 25 CFR §§502.14(d) and 502.19(d) are not categories of key employees and primary management officials whose prints can be submitted to the FBI through the NIGC MOU. However, the tribe can continue to license these categories through the NIGC if the tribe has an alternative, legal source of FBI CHRI other than the NIGC such as a statutory authorized tribal, state, local or 3<sup>rd</sup> party contractor.

1. Is the person an applicant or employee of the gaming operation?<sup>7</sup>
  - If yes, proceed to question two.
  - If no, the person cannot be fingerprinted because they do not satisfy the initial criterion of being an applicant or employee of a gaming operation.
  
2. An applicant or employee of a gaming operation whose “total cash compensation” will be or is in excess of \$50,000 per year?<sup>8</sup>
  - If yes, the person can be fingerprinted as a KE.
  - If no, proceed to the next question.
  
3. Is the person one of the “four most highly compensated persons in the gaming operation?”
  - If yes, the person can be fingerprinted as a KE.
  - If no, proceed to the next question.
  
4. A person in a position or performs duties that meet the definitions of a KE in accordance with NIGC regulation, 25 C.F.R. § 502.14 (a) through (c)?
  - If yes, the person can be fingerprinted as a KE.
  - If no, proceed to the next question.
  
5. Does the person watch, protect, handle, use, or maintain gaming cash and/or gaming revenue<sup>9</sup>? Gaming cash means money used in the operation of Class II and III gaming. This includes cash deposited or withdrawn from the gaming operation’s cage or vault, in its kiosk and atms, gaming machine/system bill acceptors, drop boxes, change boxes, tip boxes, or other locations, containers, and devices used to store or retrieve cash used for the conduct of Class II and III games or accounted for as a cash asset of the gaming operation. The fact valet, housekeeping, wait staff, and other employees not involved in the conduct of gaming routinely receive tips and place them in a tip box would not require them to be licensed, but the person collecting and depositing the cash tips in the gaming operation’s cage/vault who takes on responsibility for an asset on behalf of the gaming operation qualifies as a KE.
  - If yes, the person can be fingerprinted as a KE.
  - If no, proceed to the next question.

---

<sup>7</sup> See NIGC regulation, § 502.10, defining *Gaming operation*.

<sup>8</sup> This includes all employees on the gaming operation’s payroll, full-time or part-time. Is the employee’s compensation listed as an operating expense on the gaming operation’s general ledger? Does the gaming operation issue a W-2 to the employee? Is the employee subject to the gaming operations employee handbook, rules and leave policy? In some circumstances, all tribal employees are paid through the tribe and follow the tribal employee handbook, including gaming operation employees. Examination of organization charts maintained by the gaming operation or tribal business entities will assist in making a determination. Does the employee and/or their supervisor report to the gaming operation’s general manager or executive officer? Examining the process under which the employee was hired can be helpful. Were they processed through something other than the gaming operations HR department?

<sup>9</sup> See NIGC regulation, § 502.16, defining *Net gaming revenue*

6. Is the person a custodian of gaming supplies? This may include but is not limited to a person with access to gaming systems, machine ticket paper, chips, tokens, playing cards, bingo paper, bingo balls, or hardware/software used in conjunction with the Class II/III gaming systems.
  - If yes, the person can be fingerprinted as a KE.
  - If no, proceed to the next question.
7. Does the person have the ability to access and/or make changes to the gaming operation's accounting system, player tracking system, or gaming system record? This may include but is not limited to a person "with access to cash and accounting records," including accounting records within gaming equipment and devices.
  - If yes, the person can be fingerprinted as a KE.
  - If no, proceed to the next question.
8. Does the person have duties or responsibilities that include oversight of any portion of a gaming operation?<sup>10</sup> Oversight duties or responsibilities may include but are not limited to manager-on-duty obligations.
  - If yes, the person can be fingerprinted as a KE.
  - If no, proceed to the next question.
9. Does the person perform the function of bingo caller, count room supervisor, chief of security, floor manager, pit boss, dealer, croupier<sup>11</sup>, or approver of credit?
  - If yes, the person can be fingerprinted as a KE.
  - If no, proceed to the next question.
10. Does the person have any job functions or responsibilities that require the person to watch, touch, guard, count, maintain, or otherwise be responsible for gaming cash, gaming revenue, or gambling supplies/devices that has not already been discussed? The responsibilities may include accessing or modifying a Class II/III gaming system, player tracking system, or any other ancillary system that is integral to the play of the games or generation, collection, or recording of gaming revenue.
  - If yes, the person can be fingerprinted as a KE.
  - If no, the individual is not a KE.

#### Questions for PMO Classification

1. Is the person an applicant or an employee of a gaming operation or a management contractor?
  - If yes, proceed to question two.
  - If no, the individual cannot be fingerprinted unless they can be classified as a KE in the previous section.
2. Does the person have management responsibility for a gaming operation, facility, or part of either due to a management contract?

---

<sup>10</sup> See NIGC regulation, § 502.10, defining *Gaming operation*.

<sup>11</sup> Croupier is an employee of a gambling casino who collects and pays bets and assists at the gaming tables.

- If yes, the person can be fingerprinted as a PMO.
  - If no, proceed to next question.
3. Does the person have the ability “to hire or fire employees?”
- If yes, the person can be fingerprinted as a PMO.
  - If no, proceed to next question.
4. Does the person “set up working policy for the gaming operation?”<sup>12</sup> This can include, but is not limited to, actions that direct a person to perform operational, administrative, or financial functions for a gaming operation.
- If yes, the person can be fingerprinted as a PMO.
  - If no, proceed to next question.
5. Does the person plan, organize, or coordinate the activities of gaming operation/management contractor employees at the gaming operation?
- If yes, the person can be fingerprinted as a PMO.
  - If no, proceed to next question.
6. Is the person “the chief financial officer or other person who has financial management responsibility for the operation?”
- If yes, the person can be fingerprinted as a PMO.
  - If no, the person is not a PMO.

**Please note: The definition of key employee and primary management official has not changed. The FBI and FBI/NIGC MOU have clarified which KE and PMO applicant fingerprints can be submitted through the NIGC under the MOU.**

---

<sup>12</sup> See NIGC Bulletin 1994-5, *Approved Management Contracts v. Consulting Agreements* (Oct. 14, 1994) (describing what are management functions and duties), <https://www.nigc.gov/images/uploads/bulletins/1994-5mgmtvconsult.pdf>

# Appendix M



## 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.<sup>1</sup>

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<sup>2</sup>, 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>

---

<sup>1</sup> See 28 C.F.R. § 50.12(b).

<sup>2</sup> 25 C.F.R. § 556.2.

## **CHRI Use and Protection**

### **1. CHRI**

CHRI means information collected by criminal justice agencies about 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.

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<sup>3</sup> (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.

---

<sup>3</sup> 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.

# Appendix N

## Tribe Name

Determination of Eligibility/Suitability & Notification of Results to NIGC  
(25 USC 2710 & 25 CFR 558.2)

### I. APPLICANT INFORMATION

Employee Name \_\_\_\_\_ SSN \_\_\_\_\_ DOB \_\_\_\_\_  
Date Hired \_\_\_\_\_ or Date transferred to Key or Mgmt. Position \_\_\_\_\_  
Applicant Status:  Key Employee  Primary Management Official  Other Position \_\_\_\_\_

### II. SYNOPSIS OF BACKGROUND INVESTIGATION CONDUCTED

- Current Address & Residence History (previous 5 years)  Credit Check
- Past Employment  Proof of Self-employment
- Personal Character References  Tribal and/or District Court Record Check
- Criminal History  Verified existing and previous relationships with Indian Tribes and the gaming industry.

#### The criminal history investigation revealed:

- No record.
- Every known criminal charge brought against the applicant within the last 10 years of the date of application:  
\_\_\_\_\_  
\_\_\_\_\_
- Every felony of which the applicant has been convicted or any ongoing prosecution.  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

#### OTHER GAMING LICENSES VERIFIED

- Gaming licenses previously denied: \_\_\_\_\_
- Gaming licenses revoked, even if subsequently reinstated \_\_\_\_\_
  - Employee has never applied for another gaming license  Employee has applied for previous gaming license
  - Licensing agency: \_\_\_\_\_ License Status & Position: \_\_\_\_\_
  - Licensing agency: \_\_\_\_\_ License Status & Position: \_\_\_\_\_

### III. ELIGIBILITY DETERMINATION

Based upon the information reviewed and the investigative findings and taking into consideration the applicant's prior activities, criminal record, if any, reputation, habits and associations, the \_\_\_\_\_ Gaming Commission has determined that the above named individual:

- Should be **granted** a gaming license
- Should be granted a **conditional** gaming license for a period of \_\_\_\_\_ months.  
Condition \_\_\_\_\_
- Should be **denied** a gaming license.
  - Did not fully and correctly fill out their Tribal License application as required
  - Other \_\_\_\_\_
- Has had their license **revoked** for cause (Please attach a summary of cause for revocation)  
Revoked for \_\_\_\_\_
- Not licensed by the Tribe
- Notes related to the above determination if needed: \_\_\_\_\_

\_\_\_\_\_  
Authorized Tribal Official

\_\_\_\_\_  
Date