Revised Draft – 2021 – ALL MARKUP

Color Code:

Orange: 2017 NIGC-Tribal MOU
Blue: NIGC need
Purple: FBI / CJIS requirement
Green: Modeled after FBI TAP MOU
Brown: Modeled after NIGC-FBI MOU

Memorandum of Understanding
with the National Indian Gaming Commission
regarding Criminal History Record Information

I. Purpose

In order to assist the [list name of tribal Gaming Commissione] (~~Tribe~~TGRA) to determine the eligibility of applicants for key employee (ke) or primary management official (pmo) positions in its gaming operation(s), the National Indian Gaming Commission (NIGC) will obtain criminal history record information (CHRI) from the Federal Bureau of Investigation (FBI) on these applicants and disseminate it to the ~~Tribe's gaming regulatory authority (~~TGRA~~)~~. This Memorandum of Understanding (MOU) ~~sets forth~~memorializes the NIGC's and TGRA's understandings and ~~agreed upon~~ responsibilities ~~and functions of the parties for~~regarding the ~~submitting~~ submission of noncriminal justice fingerprints~~,~~ and the transmittal, receipt, storage, use, and dissemination of CJI and ~~ng, using, and protecting~~ CHRI~~; and the FBI and the NIGC's conditions of its release and reuse~~.

Commented [A1]: San Pasqual and Jamul comment – change to TGRA

Accepted.

Commented [A2]: Shoshone Bannock – suggested revision

Accepted.

II. Parties

This MOU is between the NIGC and the ~~Tribe~~TGRA, hereinafter referred to as "~~parties~~Parties."

Commented [A3]: Shoshone Bannock comment – suggested change

Accepted.

III. Definitions

A. CJI
Criminal Justice Information (CJI) is the term used for FBI 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. Such information includes, but is not limited to:

1. "Biometric Data— fingerprints, palm prints, iris scans, and facial recognition data;

2. Identity History Data—textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual;

3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data;

4. Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII); and

5. Case/Incident History—information about the history of criminal incidents."[1]

Commented [A4]: Shoshone Bannock comment – revise according to their suggested language

Not accepted – this language is quoted from the CJIS Security Policy (CSP Policy) at 4.1.

B. CHRI

Criminal history record information (CHRI) is a subset of CJI. As set forth in 28 C.F.R. § 20.3, 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. The term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system." CHRI also includes information that is transferred or reproduced directly from CHRI or information that confirms the existence or nonexistence of CHRI.[2] CHRI includes any media that contains it, such as: letters, emails, documents, notes, conversations – in person or via phone/text, and spreadsheets or tables.[3] Examples of CHRI potentially include notice of results (NORs), licensing objection letters, and other summaries of CHRI.

C. PII

Personally identifiable information (PII) is "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."[4]

~~C.~~D. Imminent Risk

[1] CJIS Security Policy, version 5.9 at section 4.1 (June 1, 2020) (hereinafter CSP ~~Policy~~).
[2] *See* Next Generation Identification Audit, Noncriminal Justice Access to Criminal History Record Information, Policy Reference Guide (hereinafter NGI) at 1 (Apr. 6, 2020).
[3] *Id.*
[4] *See* FBI-NIGC Memorandum of Understanding re: noncriminal justice fingerprint submissions (FBI-NIGC MOU) at VI(E) (Jan. 17, 2020).

Imminent risk is the chance or possibility of loss, damage, or a calamity, threatening to occur immediately or dangerously impending or about to take place.[5]

IV. Authorities

The NIGC ~~and the Tribe~~ enters into this MOU ~~under the NIGC's~~ pursuant to its fingerprint collection~~/~~ and background check authorities for class II and class III gaming enterprises, ~~that include~~ including ~~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),~~.~~ ~~and~~ Under 28 U.S.C. § 534(a)(1) and (4), the U.S. Department of Justice collects criminal identification, crime, and other records and may provide such information to federal government officials for their official use.[6] ~~Tribes~~ TGRAs are arms of sovereign tribal governments and enter this MOU in that capacity. TGRAs are permitted to submit fingerprints to the FBI through the NIGC to obtain and use CHRI if they have ~~an~~ executed this MOU with the NIGC.

V. Responsibilities

A. The NIGC ~~agrees to~~ will:

1. ~~Ensure~~ Pursuant to the FBI-NIGC Memorandum of Understanding re: noncriminal justice fingerprint submissions (January 17, 2020) (hereinafter FBI-NIGC MOU), provision I, ~~A~~accept fingerprint submissions ~~have been~~ that are properly and adequately completed~~.~~ for purposes of ~~the TGRA's determining an applicant's eligibility for employment and licensing as a ke or pmo at the Tribe's gaming operation, as defined in NIGC regulations.~~ 25 C.F.R. §§ 502.14(a) – (c) and 502.19(a) – (c).

2. Convert properly submitted fingerprint card submissions into an electronic format and forward them to the FBI via a means acceptable to the FBI. NIGC agrees to comply with the CJIS Security Policy (CSP).

3. Collect and remit the FBI's fee for the processing of the applicant fingerprint submission.[7]

[5] *See, e.g.*, IMMINENT and RISK, Black's Law Dictionary (11th ed. 2019).
[6] *See also* 28 C.F.R. § 20.33(a)(2) ("Criminal history record information contained in the III System and the FIRS may be made available: … (2) To federal agencies authorized to receive it pursuant to federal statute or Executive order ….").
[7] *See* 25 C.F.R. §§ 514.15 – 514.17; FBI Criminal Justice Information Services Division, User Fee Schedule, 83 Fed. Reg. 48335-01 (Sept. 24, 2018).

Commented [A5]: New definitions

Commented [A6]: Shoshone Bannock comment – revise to speak only to NIGC's authority.

Accepted.

Commented [A7]: San Pasqual and Jamul comment – clearly incorporate federal requirements rather than summarizing them.

Accepted throughout document. However, in some instances, the summary explanation remains to assist compliance by clearly stating the obligation.

Commented [A8]: Shoshone Bannock comment – each Tribe should set forth its own grounds for its sovereign authority.

Compromise language proposed.

Commented [A9]: Shoshone Bannock comment – suggested this language

Accepted.

Commented [A10]: Shoshone Bannock suggested language

Accepted.

Commented [A11]: Seminole Tribe comment – It is inappropriate for the NIGC to force the Tribe to accept FBI's legal interpretation of IGRA and/or NIGC regulations. But recognizes that the FBI and NIGC may agree on certain legal interpretations.

Accepted - Eliminated this provision in Tribal section and moved it to NIGC section.

Seminole comment 2 – Removing 502.14/19 (d) threatens the integrity of Indian gaming. NIGC has legitimate law enforcement / statutory authority for such requests. Further, NIGC should not limit its authority to disseminate CHRI to tribes in a manner that is inconsistent with its broad authority to secure information necessary for its statutory purpose.

Response – The current FBI-NIGC MOU only affords the dissemination of CHRI for 502.14/19 (a) – (c).

Commented [A12]: Shoshone Bannock comment – Add that NIGC will "ensure that submission methodology will be compliant with FBI's CSP Policy" and "maintain a log of transactions and disseminations."

Accepted in substance – NIGC agrees to comply with the CSP Policy.

Shoshone Bannock also wants NIGC to agree to report to each TGRA when their information is used, disclosed o … [1]

4. Provide the ~~Tribe~~ TGRA with a monthly accounting and assessment of fingerprint fees due by the [date] of every month.

~~5. Promptly notify tribal authorities if the NIGC determines that it must discontinue disseminating CHRI to the Tribe – either in whole or in part – due to the Tribe's failure to comply with the conditions in this MOU and/or the FBI CJIS Security Policy (Policy), which is incorporated here by reference. The NIGC agrees to do the same if it decides to suspend disseminating CHRI to the Tribe due to the Tribe's potential failure to comply with the conditions of this MOU and/or the Policy.~~

~~6.~~5. ~~Disseminate~~ CHRI to authorized TGRA representatives. Such disseminations will only contain CHRI on a particular applicant and will not contain the NIGC's recommendations or conclusions. ~~The NIGC, however, reserves the right to furnish summary memoranda that contain solely CHRI results.~~

~~7.~~6. Provide operational, technical, and investigative assistance with regards to security incidents.

~~8.~~7. Provide an authorized, secure telecommunication interface with the FBI CJIS.

~~9.~~8. Provide timely information on all aspects of the CSP, the Next Generation Identification Audit, Noncriminal Justice Access to CHRI, Policy Reference Guide (NGI) information, and other related programs by means of technical and operational updates, newsletters, and other documents~~;~~.

~~10.~~9. Pursuant to the FBI-NIGC MOU, provision VI(I), "provide appropriate training regarding the responsibilities of [the FBI-NIGC] MOU to [tribal officials] whose information sharing activities are covered by the provisions of [the] MOU." Also ~~Provide~~ provide training assistance and up-to-date materials to designated tribal officials~~;~~. ~~and~~

~~11.~~10. Pursuant to the FBI-NIGC MOU, provision VI(J), "audit the handling and maintenance of [CHRI] in electronic and paper recordkeeping systems to ensure that appropriate security and privacy protections are in place." Such ~~Audit~~ audits will occur primarily through the use of questionnaires, on-site inquiries and testing, observations, and interviews. At the NIGC's discretion, audits may ~~be unannounced or scheduled and~~ include the use of document requests.[8]

[8] *See* ~~CJIS Security Policy (CSP Policy)~~ section 5.11.

Commented [A13]: Navajo comment/suggested language

Accepted.

Commented [A14]: Shoshone Bannock comment - Move to part VI

Accepted.

Commented [A15]: Shoshone Bannock suggested language

Accepted.

Commented [A16]: Shoshone Bannock comment – We have been advised to limit the use of summary memoranda and therefore prefer not to receive any memoranda from the NIGC with CHRI results.

Accepted.

Commented [A17]: Navajo comment – The Nation is concerned about unannounced audits at NIGC's discretion and requests that NIGC provide a clear definition and procedures for the unannounced audits.

Changed to only announced audits.

~~12.~~11. Appoint the NIGC NIGC CJIS Systems Officer (CSO) as the point-of-contact for this MOU, including any issues or concerns.

B. The ~~Tribe~~TGRA will:

~~1. Agrees to and understands that the FBI retains the right to approve CHRI dissemination and, in the future, may prohibit the NIGC from disseminating CHRI.~~

~~2. Agrees to and understands that the NIGC will not release any CHRI without first having received all required prior approvals from the FBI and will not release CHRI when prohibited from doing so by the FBI.~~

~~3. Agrees to and understands that the FBI may impose additional restrictions on the dissemination and use of CHRI (in addition to those imposed by the NIGC), and that the Tribe will be subject to all such additional restrictions.~~

~~4.~~1. ~~Agrees to m~~Modify its fingerprint operating systems to meet CSP requirements and the NIGC's connectivity requirements ~~NIGC's specifications and timeframes~~, unless processing fingerprints by hard card submissions. Requests for exceptions from the NIGC's connectivity requirements may be submitted to the NIGC ISO for review and approval prior to their implementation. ~~Doing so facilitates and ensures secure access to the NIGC fingerprint system. Failing to modify or upgrade operating systems to conform to NIGC's instructions, specifications, and timeframes are grounds for NIGC suspending and/or terminating its services to the TGRA and Tribe.~~

~~5. Agrees to use CHRI solely for the purpose of determining an applicant's eligibility for employment and licensing 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.~~

~~6.~~

~~7. A~~cknowledge ~~grees to and understands that until~~ unless NIGC ~~amends its regulations~~federal law is amended, ~~fingerprints of TGRA staff and/or Commissioners cannot be submitted unless the TGRA staff and/or Commissioners are key employee~~kes of the gaming operation.

Commented [A18]: Shoshone Bannock suggested insertion

Accepted.

Commented [A19]: Shoshone Bannock suggested language.

Accepted.

In addition, Shoshone Bannock asserts that the "agrees to" language is condescending.

Language modified to remedy this concern.

Commented [A20]: Quapaw, Shoshone Bannock, & Potawatomi comments – These provisions hold the TGRAs to unknown standards that the FBI may apply at any time. Remove.

Accepted - These provisions are from the old 2017 NIGC-Tribal MOU and are not required by the new FBI-NIGC MOU. However, to ensure that all updates to FBI requirements are followed, certain provisions have been modified so that TGRAs agree to all CSP and NGI updates as well as updates to the FBI Privacy Act Statement and Notice.

Commented [A21]: Jamul, Navajo, Seminole and San Pasqual comments – provision is vague. Revise to clearly state the instructions, specifications, and timeframes.

Shoshone Bannock comment – delete provision, as there are no valid grounds for NIGC to require this provision and it is vague.

... [2]

Commented [A22]: Potawatomi & Quapaw suggested language

Accepted.

Commented [A23]: Unnecessary explanatory language.

Commented [A24]: Deleted as breach of any provision in the MOU is grounds for suspension or termination.

Commented [A25]: Seminole, Potawatomi & Quapaw comment – Tribes do not agree or accept FBI's interpretation of IGRA and NIGC regulations. Request that NIGC not make them agree to it, as it is a constructive regulatory change via the MOU. In addition, the failure

... [3]

Commented [A26]: Potawatomi & Quapaw suggested change – use "unless" rather than "until."

Accepted.

Commented [A27]: Shoshone Bannock comment – delete because TGRAs recognize that key employees of the gaming operation do not include regulatory staff.

... [4]

~~8.~~2. ~~Agrees to make~~ Make reasonable efforts to ensure that personally identifiable information (PII) ~~and fingerprint data~~ is relevant, accurate, timely, and complete before submitting it to the NIGC.[9]

~~9.~~3. In the event that either Party becomes aware of any inaccuracies in the information received from the other Party pursuant to this MOU, ~~Agrees to promptly notify~~ the information recipient will promptly notify the information provider ~~if the TGRA staff or Tribe become aware of any inaccuracies in PII or fingerprint data received from the NIGC~~so that corrective action may be taken.[10]

~~10.~~4. ~~Agrees that prior~~Comply with 28 C.F.R. § 50.12(b). Prior to taking an applicant's fingerprints, the ~~Tribe~~ TGRA will provide the applicant a copy of the Non-Criminal Justice Applicant's Privacy Rights notice and the FBI's Privacy Act Statement, in writing[11], using the most current versions of each as provided by FBI CJIS at: 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.[12]

~~11.~~ [13]

~~12.~~5. ~~Agrees that if an applicant has a FBI criminal history record, the Tribe will have~~ Comply with 28 C.F.R. § 50.12(b), having written policies and procedures in place to, at minimum, provide the applicant an opportunity to complete or challenge the accuracy of the information in their FBI criminal history record, including:

a. advising the applicant in writing of the procedure for obtaining a change, correction, or update to the record as set forth in 28 C.F.R. § 16.34;

b. affording the applicant a reasonable time to correct or complete the record (unless they explicitly decline to do so) before denying their gaming license or employment based upon the information in the record[14];

[9] *See* FBI-NIGC MOU at VI(F).
[10] *Id.* VI(G).
[11] Written notification includes electronic notification, but excludes oral notification.
[12] *See also* NGI, *supra* at 13.
~~[13] Written notification includes electronic notification, but excludes oral notification.~~
~~[14] *See* 28 C.F.R. § 50.12(b).~~

Commented [A28]: Shoshone Bannock comment – make this the same as the FBI-NIGC MOU provision.

Accepted.

Commented [A29]: Shoshone Bannock comment – Make this provision one where both the NIGC and TGRAs agree to it.
And change language to the same as the FBI-NIGC MOU at VI(F).

Response to comment – NIGC has already agreed to the provision in its MOU with FBI. The language here is not exactly the same as the MOU, but similar – as it clearly sets forth the obligations/goal of the NIGC-Tribal MOU.

c. choosing to develop written procedures for providing applicants copies of their records for review and possible challenge, correction, or update that require:

(i) Verification of the applicant's identity prior to dissemination of the copy to the applicant or an attorney working on their behalf;

(ii) Documenting the release of the copy; and

(iii) Marking the copy in some manner to distinguish it as the applicant's copy, not the original. (e.g., watermark). To be clear, the copy must not be reused for any other purpose.

d. Or, instead of sub-section (c) herein, electing not to provide applicants copies of their FBI criminal history records by developing a written policy prohibiting the release of the records for such purpose and directing applicants to the FBI's process for obtaining a copy (set forth in 28 C.F.R. §§ 16.30 – 16.34 and FBI's website, http://www.fbi.gov/about-us/cjis/background-checks).[15]

~~13. Agrees to and understands that NIGC's disseminations will only contain CHRI on a particular applicant and will not contain NIGC recommendations or conclusions. The NIGC, however, reserves the right to furnish to the Tribe and/or TGRA summary memoranda containing the CHRI results.~~

~~14.~~6. Comply with 28 C.F.R. § 20.33(d): CHRI "shall be used only for the purpose requested," 28 C.F.R. § 20.21 and CSP ~~Policy~~section 4.2.1.

~~15.~~7. Comply with NGI's Reuse standard: "not subsequently re-use CHRI for unrelated needs, even if new needs are covered by a recognized/approved authority."[16] ~~Agrees to not duplicate, disseminate, or reuse CHRI;~~This ~~including~~ includes sharing it with applicant's spouse, household, other family members, tribal leadership, tribal agencies not involved in employing or licensing ~~key employee~~kes or ~~primary management officials~~pmos, human resource departments, 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

[15] *See also* 28 C.F.R. § 20.34; NGI, *supra* at 17.
[16] NGI, *supra* at 3; *see also id.* at 4.

Commented [A30]: Shoshone Bannock Comment – delete these provisions, as Tribes/TGRAs are well aware of this obligation. Also delete because it is part of CSP Policy, which TGRAs agree to abide by.

Not accepted - As a result of FBI's NIS Audit, NIGC promised that it would incorporate this standard into its new MOU. Further, these are not CSP Policy obligations.

Comment 2 – Instead of summarizing federal requirements, simply incorporate them.

Partially accepted – NIGC concludes that the statement: "Agrees to comply with 28 CFR 50.12(b)" is vague and believes there is a benefit to clearly describing the obligations in the provisions.

Commented [A31]: Shoshone Bannock comment – move to NIGC obligation section

Accepted.

Commented [A32]: Comment – Incorporate federal requirements instead of summarizing them.

Partial acceptance – did both.

Shoshone Bannock comment **for the next 4 provisions** – delete these requirements, because the Tribe is well aware of FBI requirements and does not need to agree to them in a MOU with the NIGC. Also the agreement to abide by the CSP Policy eliminates the need for these provisions.

Not accepted – These requirements do not derive from the CSP Policy. As to the next provision, NIGC promised in its FBI NIS Audit to address reuse in the MOU.

Commented [A33]: Comment - Incorporate federal requirements instead of summarizing them.

Partial acceptance – did both. In FBI NIS Audit response, NIGC agreed to clarify this standard in its new MOU.

from the NIGC cannot be used for such purpose – a new record request to the FBI through a non-NIGC process must be made in such instance.[17]

~~16.~~8. ~~Agrees to~~ Comply with NGI's Residual Access standard: limit residual access to CHRI "to only the minimum level necessary to accomplish oversight responsibilities" by a state gaming agency (such as access to CHRI as part of an audit or review of licensing during a regulatory inspection) or by an inspector general's office.[18] And ~~agrees to~~ establish controls to reasonably prevent unauthorized CHRI disclosure.[19]

~~17. Agrees~~Ensure ~~that, except in connection with proceedings related to the Tribe's TGRA's licensing determinations for its key employees~~kes ~~and primary management officials~~pmos~~, CHRI nor any summary of it shall be reproduced, distributed, reused, or introduced in a court of law or administrative hearing without the NIGC's prior written consent. To be clear, prior NIGC written consent is not necessary for the purposes set forth in 10~~5(c) ~~and 13~~ 8 ~~above or for purposes of a ke or pmo applicant's licensing or employment appeal hearing.~~

~~18. Comply with CSP Policy, section 5.1.3 and Agrees to document each release of a criminal history record, CJI, or CHRI in a dissemination log, meaning copies of a record released to an applicant, an applicant's attorney, or for purposes of an applicant's licensing or employment appeal hearing. This log shall include:~~

~~a. Date of Dissemination.~~
~~b. Applicant's Name.~~
~~c. Provider's Name (Released By).~~
~~d. Requestor's Name & Released To.~~
~~e. SID/FBI Numbers.~~
~~f. Reason for Dissemination (Why was this information requested? For what purpose?).~~

~~How the information was disseminated (email, fax, certified mail, etc.).~~

~~19.~~9. ~~Agrees to provide~~ Set forth on the Notice of Results (NOR), the job title or position of the ~~key employee~~ke or ~~primary management official~~pmo so that the

[17] *Id.*
[18] *Id.* at 10.
[19] *Id.*

Commented [A34]: Shoshone Bannock comment – delete provision because already captured by CSP Policy.

Accepted – Although this provision is not part of the CSP Policy, it is removed because it derives from old 2017 NIGC-Tribal MOU and is not required by the new FBI-NIGC MOU or other standards. Also, proper use and reuse of CHRI is addressed in provisions above and using it in a licensing or employment hearing is addressed in Appendix / CSP Policy.

Commented [A35]: Shoshone Bannock comment – delete because part of CSP policy, which TGRAs agree to below.

Accepted – moved to the Appendix

Commented [A36]: Shoshone Bannock Comment – delete because part of CSP Policy.

Not accepted – these standards are not part of the CSP Policy but the NGI Audit Policy Reference Guide. Moreover, NIGC explicitly promised FBI it would clarify the reuse standard in the new MOU.

NIGC may confirm that such job title/position comes within the perimeters for the NIGC to request CHRI from the FBI.

10. Acknowledge the NIGC's obligation under the FBI-NIGC MOU, provision VI(J), and provide ~~Agrees to grant~~ NIGC representatives ~~complete~~ access to CHRI ~~pertaining to kes and pmos~~ that was obtained through this MOU for purposes of inspection and/or audit to ensure compliance with this MOU.

11. If an arm of a self-regulation tribe, ~~agree to~~ grant NIGC representatives ~~complete~~ access to Class II tribal background investigation and licensing files. ~~All other tribes acknowledge that NIGC representative possess such access, as provided by NIGC regulation, 25 C.F.R. § 558.3(e). All tribes also recognize that NIGC has access to Class III tribal background and licensing files as set forth in IGRA and the same regulation. And~~ Finally,

~~20.~~12. ~~all tribes agrees that the FBI and/or NIGC may audit the handling and maintenance of information relevant to this MOU in electronic and paper form as well as in recordkeeping systems to ensure that appropriate security and privacy protections are in place. The Tribe agrees~~ Agree to fFully cooperate with ~~such~~ NIGC audits as described in provision VI(A)(10) of this MOU.

~~21.~~13. ~~Agrees to n~~Notify the NIGC, on a monthly basis, of ~~all~~ the following licensing information associated with the dissemination of CHRI for a fingerprinted applicant that does not result in a submission of a NOR: a) the reason for the fingerprint submission and b) if the submission was in error, the steps taken to correct the process that created the error. ~~permanent employees (employed more than 90 days) whose fingerprints were submitted to the NIGC for CHRI.~~

14. ~~Agrees to c~~Comply with the FBI CJIS Security Policy (CSP ~~Policy~~) and all annual updates to it, currently found at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center . An appendix attached to this MOU outlines the present primary requirements of the ~~Policy~~CSP.

~~22.~~15. Comply with the NGI and all annual updates to it.

~~Agrees to eEmploy a formal sanctions process for personnel that fail to comply with information security policies and procedures, including those mandated by the CJIS Security Policy (CSP Policy).~~

Commented [A37]: Shoshone Bannock comment – explain the basis for this provision

Accepted.

Commented [A38]: Jamul comment – contends that this appears to expand NIGC's authority and access to records that it would not otherwise possess under Federal law. Recommends deleting "complete" and only limiting access to that "necessary to ensure compliance with requirements of this MOU and applicable federal requirements."

Accepted – FBI-NIGC MOU at VI(J) requires NIGC to audit handling and maintenance of CHRI.

Shoshone Bannock comment – it is overly broad to afford NIGC "complete access to CHRI." Suggested revision to mirror language in FBI-NIGC MOU (VI)(J).

Response – Deleted the term "complete" and limited NIGC's access to CHRI that was provided pursuant to this MOU. If the CHRI is no longer in existence, NIGC does not need access to it.

Commented [A39]: Deleted, to be consistent with deletion in 11.

Commented [A40]: San Pasqual and Jamul comment – delete as it appears to expand NIGC authority.

Response – This provision is now limited to self-regulated tribes.

Commented [A41]: Quapaw, Potawatomi, and Jamul comments – request a specific explanation as to why this is needed and when the NIGC would need such access.

Deleted - because this is already is law, contained in NIGC regulations.

Commented [A42]: Quapaw & Potawatomi comments – make this provision more specific because the description – "all licensing information" – is vague and overly broad. Instead, add a list of what is required.

Accepted.

Commented [A43]: Shoshone Bannock Comment – remove because already required by the CSP Policy.

Accepted.

~~23.~~16. ~~Agrees~~Ensure that if and when the ~~Tribe's~~ TGRA's Local Agency Security Officer (LASO) changes, the new LASO will review a copy of this MOU within ~~five~~ ten business days of assuming the position as well as notify the NIGC Information Security Officer (ISO) (iso@nigc.gov) of their name and contact information within that timeframe.

VI. Effective date, Suspension, Modification, and Termination

A. Term of MOU

1. This MOU may be executed in one or more counterparts. Each shall constitute an original. A signature produced by facsimile shall be deemed an original signature and shall be effective and binding for purposes of this MOU.

~~1.~~2. This ~~agreement~~MOU shall become effective ~~when executed by~~upon the signature of both Parties and will ~~continue~~remain in effect until terminated. To be clear, this agreement remains in effect regardless of personnel changes to the Parties' signatories below.

B. Modification

1. This ~~agreement~~ MOU may be modified at any time by written consent of both Parties.

2. If the Parties desire to modify this MOU, they will provide written notification to the other Party at least thirty (30) days prior to the requested modification.

~~2.~~3. A written amendment to this MOU shall be effective upon the signature of both Parties.

C. Suspension

1. The NIGC may suspend the performance of services under this agreement if it determines that the ~~Tribe and/or its~~ TGRA has ~~potentially~~ breached any term of it.

2. CHRI dissemination to the ~~Tribe~~ TGRA will cease upon suspension of services.

Commented [A44]: Eastern Band comment – change this to 10
Cherokee comment – change to two weeks

Accepted.

Commented [A45]: Same comment as above – to delete because it's a CSP requirement.

Not accepted – Not a CSP requirement. But modelled after the DOJ-Tribal TAP MOU that contains a 5 day requirement.

Commented [A46]: Quapaw comment – add "a dispute resolution provision to address the many ambiguous provisions and standards in the MOU."

Not accepted – The vast majority of comments have been accepted to clarify the standards in this MOU.

Navajo comment – Include "a dispute resolution process in regards to any of the parties' failures in terms of the agreement."

Shoshone Bannock comment – Add our recommended dispute resolution language, which first requires informal government-to-government discourse.

Not accepted – The suspension provision has been revised. Dispute resolution is unnecessary since in most instances a TGRA will receive a 30-day notice of suspension and the issues to correct prior to the suspension occurring. The only exception is a situation of imminent risk, which is defir ... [5]

Commented [A47]: Shoshone Bannock suggested language

Accepted.

Commented [A48]: New language

Commented [A49]: Shoshone Bannock comment: Change language to – "This MOU shall become effective on the date of signature and will remain in effect unless terminated in who, or in part, by mutual agreement. Any party may ... [6]

Commented [A50]: Shoshone Bannock comment: Add new section that states "Modifications to the MOU may be made at any time by mutual consent of the Parties."

Accepted in substance. ... [7]

Commented [A51]: Shoshone Bannock comment - Add "A written amendment, signed and dated by the relevant Parties, shall be executed prior to the changes becoming effective." ... [8]

Commented [A52]: Quapaw & Potowatomi comment – remove this word, as a potential breach is overly vague and ambiguous.

Accepted.

3. The NIGC will provide written notice of such suspension to the ~~Tribe~~ TGRA at least thirty (30) days prior to the suspension along with a description of all issues that require correction or rectification prior to services being restored, unless, the NIGC has a reasonable basis for concluding that CHRI is at imminent risk and such circumstances warrant immediate suspension.

4. Upon notice under C(3), the TGRA may request an additional 30 days to respond, ~~or~~ remedy the breach or submit a written plan of action ~~which~~that addresses the breach within a~~n agreed upon~~ time frame agreed upon with the NIGC.

D. Termination

1. The NIGC will promptly notify the TGRA if the NIGC ~~determines~~concludes that it must ~~discontinue~~cease disseminating CHRI to it ~~, either in whole or in part,~~ due to the ~~Tribe~~TGRA's failure to comply with ~~the~~any condition~~s~~ of this MOU ~~and/or the FBI CJIS Security Policy (CSP Policy), which is incorporated here by reference~~. The NIGC will provide written notice of the termination to the TGRA at least thirty (30) days prior to it.

2. The TGRA may terminate this MOU, at any time, upon written notice of withdrawal to the NIGC. If the TGRA desires to terminate this MOU, it will provide written notification to the NIGC at least thirty (30) days prior to termination.

3. In the event of termination, the following rules apply:
   a. The ~~parties~~ Parties will continue participation, financial or otherwise, through the effective date of termination;
   b. All information and rights therein received under the provisions of this ~~agreement~~ MOU prior to the termination will be retained by the ~~parties~~Parties, subject to the provisions of this ~~agreement~~MOU; and
   c. CHRI dissemination to the ~~Tribe~~ TGRA will cease on ~~or before~~ the date of termination, unless suspended prior to such date due to the existence of imminent risk.

~~VII. Tribal Acknowledgment~~

Commented [A53]: New language. Also "imminent risk" is now defined in the definitions section.

Shoshone Bannock comments – In addition to the 30-day notice, requests an additional 30 days to remedy violations.

Accepted.

Commented [A54]: Shoshone Bannock comment – suggests the following grounds for termination: repeated failure to adhere to CSP Policy; repeated disregard for federal laws, regulations or orders; and substantial breach of MOU

Not accepted - because the NIGC suspension and termination provisions provide fair processes. In addition, the NIGC has added a provision to allow TGRAs to request additional time to correct a violation in the context of a suspension.

Commented [A55]: San Pasqual and Jamul comment on previous provision which allowed either Party to terminate the MOU for any reason – Access to CHRI is critical and therefore should only be terminated for violation of the MOU or federal requirements.

Accepted – provision modified. See provision directly above.

Commented [A56]: Quapaw and Potowatomi comment – remove

Accepted

Commented [A57]: New language

~~The Tribe~~ TGRA ~~acknowledges and consents to the above stated requirements and conditions of this MOU on this _____ day of _____, 20_____. It specifically acknowledges that potential failure to comply with the requirements may subject the Tribe~~ TGRA ~~to suspension of services and/or that failure to comply with the requirements may result in termination of services.~~

Agreed to by:

_____ and National Indian Gaming Commission
Name of TGRA Office ~~Tribe~~

_____ _____
Name of Authorized ~~Tribal~~ TGRA Official (PRINT) Name of Authorized NIGC Official (PRINT)

_____ _____
Signature of Authorized ~~Tribal~~ TGRA Official Official

Signature of Authorizing NIGC

(NIGC CJIS Systems Officer)

_____ _____
Date Date

_____
Name of ~~Authorized TGRA Official~~ TGRA's LASO, memorializing receipt of a copy of this MOU

Commented [A58]: Shoshone Bannock comment – Delete. There are no grounds for including this provision in the MOU.

Accepted – it is duplicative

Appendix: CJIS Security Policy – summary of primary requirements

In the MOU, the Tribe agreed to comply with the FBI CJIS Security Policy (Policy). The entire Policy may be found at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

To aid the Tribe in complying with the Policy, the following summarizes its primary requirements:

1. Local Agency Security Officer (LASO) –

   a. The Tribe or TGRA shall appoint a LASO to function as the point of contact for security and audit related issues.

   b. The LASO shall coordinate Policy compliance for the TGRA and undertake the duties set forth in Policy section 3.2.9, including establishing and maintaining a current list of authorized personnel with access to CHRI (sections 5.5.2 & 5.5.2.4); providing that list to the NIGC Information Security Officer (ISO) (iso@nigc.gov); updating the list when changes occur; and providing the updated list to the NIGC ISO also when changes occur (http://bit.ly/AUserList).

   c. The LASO will complete the required training set forth in Policy section 5.2.2 prior to assuming duties and annually thereafter.

2. Non-Channeler Outsourcing Standard –

   a. Outsourcing that allows an external entity to access CJI and/or CHRI obtained or maintained by the Tribe's TGRA is not permitted without an FBI-approved non-channeler outsourcing contract.

   The TGRA must obtain the FBI CJIS Compact Officer's written approval prior to entering into an outsourcing contract or granting limited CJI or CHRI access to another entity (other than the Tribe's TGRA) for purposes of creating or maintaining the computer system(s) needed to accept or house the CHRI.[1] For such purpose, the TGRA shall send the the FBI CJIS Compact Officer a letter requesting approval and a copy of all proposed contracts, with

[1] CJIS Security Policy (Policy) section 5.1.1.7.

a copy to the NIGC ISO (iso@nigc.gov). All proposed and approved contracts must require third parties to implement standards as stringent as those in 28 C.F.R. part 906, specifically Section 906.2(c) and provide evidence that they in fact do so.

3. Security Awareness Training –

    a. The TGRA shall ensure that all persons who - access, process, read, maintain CJI and/or CHRI or the systems used to process, transmit, or store CJI / CHRI or have unescorted access to a secure location with CJI / CHRI - complete the appropriate level 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.

    b. This security awareness training must be completed for all individuals identified in the paragraph above within six (6) months of executing the NIGC MOU and all new employees within six (6) months of being assigned the duties or having access and biennially thereafter. The TGRA will document each instance when its employees receive this training and retain documentation for a minimum of two (2) years.

4. Security Incident Response –

    a. The TGRA shall create and keep current an Incident Handling policy, in accordance with CSP section 5.3, which outlines response procedures for all security incidents relating to CJI / CHRI and the system(s) used to access, store, and transmit them. This policy must include incidents involving employees, contractors, and third party users.

    b. The procedures shall include incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery[2] as well as tracking and documenting each incident, including user response activities.[3]

[2] Policy section 5.3.2.1.
[3] Policy section 5.3.4.

c. Within six (6) months of executing the NIGC MOU, the LASO shall implement the Incident Handling procedures, reporting incidents to the NIGC ISO (iso@nigc.gov), using Policy Appendix F.1, Security Incident Response Form.

d. Initial reports of security incidents shall be made to NIGC ISO (iso@nigc.gov) **within 24 hours of detection**.

5. Media Protection –

a. The TGRA shall create and keep current a policy and procedures for securing CJI and CHRI media (electronic or paper/hard copy) from unauthorized access or disclosure in accordance with Policy section 5.8.

b. The procedures shall require securely stored CJI and CHRI media. Specifically, digital and physical media must be stored in secure locations or controlled areas that are restricted to authorized personnel. If physical and personnel restrictions are not feasible then the CJI and CHRI shall be encrypted per Policy section 5.10.1.2 (FIPS 197 certified).

c. The procedures should require encryption of transported digital media at FIPS 140-2 certified. If encryption is not feasible, physical controls to ensure the security of the data, including tangible data, must be instituted.

d. The TGRA must document its compliance with the policy and procedures. Internal audit records, documenting audits of the TGRA's implementation of and compliance with the policy and procedures, must be retained for at least one (1) year. Unless otherwise specifically stated in the Policy, other documents demonstrating compliance with the policy and procedures must be maintained in accordance with the TGRA or Tribe's records retention and internal audit schedule.

e. The TGRA will destroy CJI and CHRI in accordance with Policy section 5.8 by:

i. overwriting at least three (3) times or degaussing digital media prior to disposal or release for reuse by unauthorized individuals;

ii. shredding, cutting up, or incinerating inoperable digital media and physical media;

iii. maintaining written documentation, in accordance with the TGRA or Tribe's records retention and internal audit schedule, of the steps taken to sanitize or destroy electronic and physical media; and

iv. having all media destroyed by - or witnessed by - tribal personnel with authorized access to CJI and CHRI, including when destruction is contracted to a third party company.

6. Access Control –

    a. The TGRA shall create and implement a physical protection policy and procedures in accordance with Policy section 5.5 to ensure that CJI, CHRI, and information system hardware, software, and media that contain, access, or transmit them are physically protected through access control measures.

        i. The policy shall incorporate, comply, and implement the requirements of Policy sections 5.5.1 – 5.5.2.4 and 5.5.4 – 5.5.6.2.

7. Controlled Area –

    a. The TGRA shall designate and prominently post secure areas for accessing, processing, and storing CJI and CHRI. Access to such areas shall be limited to authorized personnel only during CJI / CHRI access, transmitting, and/or processing. When unattended, the secure area, room, or storage container shall be locked.

    b. The TGRA must maintain a list of authorized personnel with access to CJI and CHRI or shall issue credentials to authorized personnel.

    c. The TGRA must control all physical access points and shall verify individual access authorizations before granting access. Unauthorized persons must be escorted by authorized personnel at all times in secure locations.

    d. Information system devices that display CJI/CHRI shall be positioned to prevent unauthorized individuals from accessing and viewing CJI/CHRI.

8. Formal Audits and Audit Record Retention –

a. The TGRA must conduct an internal audit of its compliance with the NIGC MOU and the Policy.

b. The TGRA will be subject to annual audits, including information technology security audits, by NIGC to ensure compliance with the MOU and the Policy and must fully cooperate with the audits.

c. The TGRA must implement audit and accountability controls to ensure its information systems generate audit records for significant information system security events, specifying which system components carry out auditing activities.

d. The TGRA shall produce system-generated audit records - at the application and/or operating system level - that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events, and time stamps. If an automated system is not used, manual recordings must occur. These records shall be retained for at least one (1) year. The TGRA must periodically review and update the list of defined auditable events in accordance with Policy sections 5.4.1.1 and 5.4.1.1.1.

e. The TGRA's information system shall provide alerts to the LASO in the event of an audit processing failure (e.g., software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reach or exceeded).

f. The TGRA shall designate an employee/position to review and analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to the LASO ~~and NIGC ISO (iso@nigc.gov)~~ **within 24 hours**, and to take necessary actions. This audit must be conducted at a minimum once a week.

g. The TGRA, along with NIGC, may be selected for a triannual audit by FBI CJIS staff.[4]

9. Personnel Security – If the state in which a TGRA/Tribe's personnel access CHRI has enacted state law mandating fingerprint-based records checks for non-criminal justice access to criminal history information and the Tribe has a legal means to obtain fingerprint-based records check for its personnel through such process, the Tribe will

Commented [A59]: Eastern Band and Cherokee comments – change to 48

Response – Changed to report only to the LASO.

[4] Policy sections 5.11.1.1 and 5.4.6.

ensure these checks are performed. Please note that not all states require it and not all tribes have legal means to obtain it.[5]

10. Identification and Authentication –

    a. The TGRA shall ensure access to systems and networks used to process, store, or transmit CJI/CHRI require individual authentication to verify that a user is authorized access to such information. This includes persons who administer and maintain these systems and networks. Unique identifiers may take the form of a full name, badge number, serial number, or other unique alphanumeric identifier.

    b. The TGRA agrees that all authorized users will uniquely identify themselves **before** the user is allowed to perform any actions on the system.

    c. The TGRA shall ensure that all user IDs belong to currently authorized users and keep current identification data by adding new users and disabling or deleting former users.

    d. Passwords shall meet standards in Policy section 5.6.2.1.

    e. The TGRA shall establish an identifier and authenticator management process in accordance with Policy section 5.6.3.

11. Configuration Management –

    a. The TGRA shall maintain a current complete network topological diagram in accordance with Policy section 5.7.1.2, depicting the interconnectivity of its systems and networks used to process, transmit, or store CJI/CHRI.

    b. The TGRA shall protect the diagram from unauthorized access in accordance with Policy section 5.5. During the audit process, the TGRA shall provide the diagram to NIGC and/or FBI.

12. System and Communications Protection and Information Integrity – The TGRA shall implement the proper safeguards to ensure the ~~confidentially~~ confidentiality and integrity of CJI and CHRI in accordance with Policy section 5.10, including but not be limited to:

[5] Policy section 5.12.

a. Encrypting data during transmission (FIPS 140-2 certified) and at rest outside the boundary of the physically secure location (FIPS 197 certified).
b. Implementing firewalls.
c. Using intrusion detection tools.
d. Using separate Virtual Local Area Network for voice over internet protocol.
e. Adhering to proper patch management.
f. Using software to detect and eliminate malware, spam, and spyware.

13. Mobile Devices –

a. The TGRA shall develop security controls for mobile devices allowing access to CJI and CHRI in accordance with Policy sections 5.13.2 - 5.13.4 and 5.13.7. Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI data at any time.

b. The TGRA shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios in accordance with Policy section 5.13.5. Special reporting procedures for mobile devices shall apply in the following situations:

    i. Loss of device control. For example:

        1. Device known to be locked, minimal duration of loss
        2. Device lock state unknown, minimal duration of loss
        3. Device lock state unknown, extended duration of loss
        4. Device known to be unlocked, more than momentary duration of loss

    ii. Total loss of device
    iii. Device compromise
    iv. Device loss or compromise outside of the United States.

14. Dissemination Log —

a. The TGRA shall document each release of a criminal history record, CJI, or CHRI in a dissemination log in accordance with ~~Policy~~CSP section 5.1.3, such as copies of a record released to an applicant, an applicant's attorney, or for purposes of an applicant's licensing or employment appeal hearing. This log shall include:

i. Date of Dissemination.
ii. Applicant's Name.
iii. Provider's Name (Released By).
iv. Requestor's Name & Released To.
v. SID/FBI Numbers.
vi. Reason for Dissemination (Why was this information requested? For what purpose?).
~~v.~~vii. How the information was disseminated (email, fax, certified mail, etc.).

~~14.~~15. Formal Sanctions Process

a. Employ a formal sanctions process for personnel that fail to comply with information security policies and procedures, ~~including those mandated by the~~in accordance with CSP section 5.12.4.

Commented [A60]: Comment – delete in body of MOU because this is part of the CSP policy, which TGRAs agree to in the MOU.

Accepted – moved to the Appendix

Commented [A61]: Same comment as above.

Page 3: [1] Commented [A12] **Author**

Shoshone Bannock comment – Add that NIGC will "ensure that submission methodology will be compliant with FBI's CSP Policy" and "maintain a log of transactions and disseminations."

Accepted in substance – NIGC agrees to comply with the CSP Policy.

Shoshone Bannock also wants NIGC to agree to report to each TGRA when their information is used, disclosed or accessed in an unauthorized manner, including information losses or breaches. The Tribe contends that because the NIGC has agreed to that in its FBI-NIGC MOU, it should agree to it here.

Not accepted - TGRAs do not produce CHRI, only the FBI does. Therefore, the NIGC– and accordingly the TGRAs (as a related agencies) – must inform FBI when its CHRI is accessed, etc. in an unauthorized manner.

Page 5: [2] Commented [A21] **Author**

Jamul, Navajo, Seminole and San Pasqual comments – provision is vague. Revise to clearly state the instructions, specifications, and timeframes.

Shoshone Bannock comment – delete provision, as there are no valid grounds for NIGC to require this provision and it is vague.

Accepted Jamul, Navajo, Seminole and San Pasqual comments.

Page 5: [3] Commented [A25] **Author**

Seminole, Potawatomi & Quapaw comment – Tribes do not agree or accept FBI's interpretation of IGRA and NIGC regulations. Request that NIGC not make them agree to it, as it is a constructive regulatory change via the MOU. In addition, the failure to include subsections 502.14/502.19(d) causes hardships on the TGRAs in conducting investigations on thousands of gaming employees.

Work around for first comment – See V(A)(1) – NIGC will only accept fingerprint submissions that fit within 502.14(a)-(c) and 502.19(a)-(c). Thus, based upon its MOU with FBI, the limitation is imposed on the NIGC and what it will accept for processing.

Page 5: [4] Commented [A27] **Author**

Shoshone Bannock comment – delete because TGRAs recognize that key employees of the gaming operation do not include regulatory staff.

Seminole comment –removing background checks on regulatory staff introduces risks to the integrity of gaming operations. The NIGC has a legitimate law enforcement / statutory purpose for such requests and not including that here negates such authority. Moreover, Congress gave NIGC broad authority to request information necessary to carry out IGRA.

Accepted Shoshone Bannock comment.

Page 10: [5] Commented [A46] Author

Quapaw comment – add "a dispute resolution provision to address the many ambiguous provisions and standards in the MOU."

Not accepted – The vast majority of comments have been accepted to clarify the standards in this MOU.

Navajo comment – Include "a dispute resolution process in regards to any of the parties' failures in terms of the agreement."

Shoshone Bannock comment – Add our recommended dispute resolution language, which first requires informal government-to-government discourse.

Not accepted – The suspension provision has been revised. Dispute resolution is unnecessary since in most instances a TGRA will receive a 30-day notice of suspension and the issues to correct prior to the suspension occurring. The only exception is a situation of imminent risk, which is defined in the agreement. Termination also requires a 30-day notice and CHRI will still be distributed unless there is imminent risk.

Page 10: [6] Commented [A49] Author

Shoshone Bannock comment: Change language to – "This MOU shall become effective on the date of signature and will remain in effect unless terminated in who, or in part, by mutual agreement. Any party may withdraw from the MOU by providing thirty days' written notice to the other Party."

Accepted in part.

Page 10: [7] Commented [A50] Author

Shoshone Bannock comment: Add new section that states "Modifications to the MOU may be made at any time by mutual consent of the Parties."

Accepted in substance.

Navajo comment – Recommend "an annual term period to allow for revisions and updates due to law and regulation amendments and changes to be fully incorporated in a new MOU and close previous MOUs."

Not accepted – Unnecessary since the NIGC will alert TGRAs via a 30-day notice to the necessity of changes in law and/or regulation that require a new MOU.

Page 10: [8] Commented [A51] Author

Shoshone Bannock comment - Add “A written amendment, signed and dated by the relevant Parties, shall be executed prior to the changes becoming effective.”

Accepted in substance.