Final MOU– ALL MARKUP

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 Commission] (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 TGRA. This Memorandum of Understanding (MOU) memorializes the NIGC's and the TGRA's understandings and responsibilities regarding the submission of noncriminal justice fingerprints and the transmittal, receipt, storage, use, and dissemination of CJI and CHRI.

II. Parties

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

III. Definitions

Commented [A1]: Seneca Cayuga Nation – Add definitions to this section for the applicable NIGC officers/employees with whom TGRAs will be in contact. Specifically, CSO and ISO, clarifying when it is appropriate or necessary for a TGRA to contact each.

Response – Accepted in part. Added these definitions to the Appendix, because that is where LASO is defined.

A. CJI
Criminal Justice Information (CJI) is the term used for 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. 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]

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]

D. Imminent Risk

Imminent risk is the chance or possibility of non-compliant or unauthorized handling, maintenance, use, disclosure of —or access to— CHRI, threatening to occur immediately or dangerously impending or about to take place.[5]

IV. Authorities

The NIGC enters into this MOU pursuant to its fingerprint collection and background check authorities for class II and class III gaming enterprises, including: 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).

---

[1] CJIS Security Policy, version 5.9 at section 4.1 (June 1, 2020) (hereinafter CSP).
[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).
[5] *See, e.g.,* IMMINENT and RISK, Black's Law Dictionary (11th ed. 2019).

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] The TGRAs are arms of sovereign tribal governments and enter this MOU in that capacity. The TGRAs are permitted to submit fingerprints to the FBI through the NIGC to obtain and use CHRI if they have executed this MOU with the NIGC.

V. Responsibilities

A. The NIGC will:

1. Pursuant to the FBI-NIGC Memorandum of Understanding re: noncriminal justice fingerprint submissions (January 17, 2020) (hereinafter FBI-NIGC MOU), provision I, accept fingerprint submissions that are properly and adequately completed for purposes of 25 C.F.R. §§ 502.14(a) – (c) and 502.19(a) – (c). If the NIGC amends its regulations to permit the fingerprinting of new or additional categories of primary management officials and/or key employees, this MOU will apply to the NIGC's acceptance of their fingerprints and the resulting CHRI upon the regulations' effective date.

2. Convert properly submitted fingerprint card submissions into an electronic format and forward them to the FBI via a means acceptable to the FBI. The 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]

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

5. Disseminate CHRI to the authorized TGRA representatives after receipt of it from the FBI. Such disseminations will only contain CHRI on a particular applicant ~~and will not contain the NIGC's recommendations or conclusions~~.

Commented [A2]: Added for clarification

Commented [A3]: Seneca Cayuga Nation – Requests that NIGC clarify when TGRAs can expect 1) CHRI disseminations and 2) any recommendations or conclusions related to an applicant for KE or PMO license.

Response: Accepted. Clarified.

[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).

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

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

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.

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 training assistance and up-to-date materials to designated tribal officials.

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 audits will occur primarily through the use of questionnaires, on-site inquiries and testing, observations, and interviews. At the NIGC's discretion, audits may include the use of document requests.[8]

11. Appoint the NIGC CJIS Systems Officer (CSO) as the point-of-contact for this MOU, including any issues or concerns. The NIGC CSO may be contacted by email at CSO@nigc.gov and by telephone at (202) 632-7003.

12. Promptly notify the TGRA of any impending FBI audit, after being provided notice of that audit by the FBI.

B. The TGRA will:

1. Modify its fingerprint operating systems to meet CSP requirements and the NIGC's connectivity requirements. Requests for exceptions from the NIGC's connectivity requirements may be submitted to the NIGC ISO for review and approval prior to their implementation. If fingerprints are processed by hard card submissions, they are exempt from the requirements outlined in this provision.

[8] *See* CSP section 5.11.

Commented [A4]: Seneca Cayuga Nation – TGRAs need to be aware of who is serving as NIGC's CSO and ISO, their contact information, as well as when NIGC personnel in these roles change.

Response – Accepted in part. Names of the NIGC CSO and ISO are not necessary, as the contact information supplied will put TGRAs in contact with the appropriate NIGC employees.

Commented [A5]: Prairie Band Potawatomi – Other requirements central to preserving the security of CHRI should be highlighted in this section too. For example, the circumstances and timeline for TGRAs to report security incidents to the NIGC and/or FBI.

Response – Not accepted. As to adding other detailed provisions, several other tribes previously requested that they be removed and replaced with a general directive that Tribes abide by the CSP.

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

3. In the event that either Party becomes aware of any inaccuracies in PII received from the other Party pursuant to this MOU that would impact the Party's ability to assess employment or licensing eligibility, the information recipient will promptly notify the information provider so that corrective action may be taken.[10]

4. Comply with 28 C.F.R. § 50.12(b). Prior to taking an applicant's fingerprints, the 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]

5. 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;

    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

[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.

(iii) Marking the copy in some manner to distinguish it as the applicant's copy, not the original. (e.g., watermark). 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 the FBI's website, http://www.fbi.gov/about-us/cjis/background-checks).[13]

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 section 4.2.1.

7. Comply with NGI's Reuse standard: do "not subsequently re-use CHRI for unrelated needs, even if new needs are covered by a recognized/approved authority."[14] This standard prohibits sharing it with applicant's spouse, household, other family members, tribal leadership, tribal agencies not involved in employing or licensing KEs or PMOs, human resource departments, potential employers, and state gaming or licensing agencies. Even if the use of CHRI may be necessary to satisfy state licensing requirements, CHRI 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.[15]

8. 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.[16] And establish controls to reasonably prevent unauthorized CHRI disclosure.[17]

9. Set forth on the Notice of Results (NOR), the job title or position of the KE or PMO so that the NIGC may confirm that such job title/position comes within the perimeters for the NIGC to request CHRI from the FBI.

---

[13] *See also* 28 C.F.R. § 20.34; NGI, *supra* at 17.
[14] NGI, *supra* at 3; *see also id.* at 4.
[15] *Id.*
[16] *Id.* at 10.
[17] *Id.*

Final MOU– ALL MARKUP

10. Acknowledge the NIGC's obligation under the FBI-NIGC MOU, provision VI(J), and agrees to provide the NIGC representatives access to CHRI 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, grant the NIGC representatives access to the Class II tribal background investigation and licensing files corresponding with the CHRI that was obtained through this MOU for the purposes outlined in #10 of this section.

12. ~~Fully c~~Cooperate to schedule and conduct ~~with~~ NIGC audits ~~as described in~~consistently with provision V(A)(10) of this MOU.

13. Notify the NIGC, on a monthly basis, of 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.

14. Comply with the FBI CJIS Security Policy (CSP) 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 CSP.

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

16. Ensure that if and when the TGRA's Local Agency Security Officer (LASO) changes, the new LASO will review a copy of this MOU within 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.

17. Comply with this MOU as to new or additional categories of primary management officials and/or key employees~~,~~ by the regulatory effective date, if they are added to NIGC regulations.

VI. Effective date, Suspension, Modification, and Termination

Commented [A6]: Prairie Band Potawatomi – Clarify this provision by rephrasing it.

Response - Accepted

Commented [A7]: Prairie Band Potawatomi – This provision is vague as to the applicable standard that will apply because the term "full" in relation to cooperation is relative and therefore subjective. The Nation recommends revising this provision to read: "Both Parties will cooperate to schedule and conduct the NIGC audits consistently with provision V(A)(10) of this MOU."

Response – Accepted in part.

Commented [A8]: Added for clarification.

Commented [A9]: Chickasaw Nation – These requirements are indefinite and indeterminate in their proposed application to new or additional categories of pmos and/or kes. These categories have not been created or properly vetted through the comment process. Any changes to regulation that are applicable to this MOU should require a new or revised MOU between the NIGC and TGRAs.

Response – The Commission intends to consult on these potential regulatory changes this month. Via consultation and the rulemaking process, tribes will have the opportunity to weigh in on them. Moreover, this paragraph does not require compliance with any new or additional regulatory provision until its effective date.

Final MOU– ALL MARKUP

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.

2. This MOU shall become effective upon the signature of both Parties and will remain in effect until terminated, regardless of personnel changes to the Parties' signatories below.

B. Modification

1. This 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.

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 TGRA has breached any term of it.

2. CHRI dissemination to the TGRA will cease upon suspension of services. During this time period:

   a. The TGRA may use CHRI that was already communicated/received for IGRA purposes —employment and licensing of PMO and KE;
   b. CHRI requested prior to the suspension of services will automatically be communicated to the TGRA upon restoration of services; and
   c. Suspension of services does not impact NIGC's regulatory requirements and deadlines.

3. The NIGC will provide written notice of such suspension to the 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 time period to remedy the breach or submit a written plan of action that remedies the breach within a time period agreed upon with the NIGC. NIGC will review the TGRA's request, approving, modifying, or denying it.

D. Termination

1. The NIGC will promptly notify the TGRA if the NIGC concludes that it must cease disseminating CHRI to it due to:
   a. the TGRA's inability to remedy a breach of any term of this MOU within the time period set forth in C(3) (if the TGRA does not submit a request under C(4), above) or within the time period set forth in C(4);
   b. a second suspension under C due to a finding of imminent risk; or
   c. a third suspension under C.

2. The NIGC will provide written notice of the termination to the TGRA at least thirty (30) days prior to such termination.

3. 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.

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

Agreed to by:

_____ and National Indian Gaming Commission

Final MOU– ALL MARKUP

Name of TGRA Office

_____	_____
Name of Authorized TGRA Official (PRINT) (PRINT)	Name of Authorized NIGC Official
_____	_____
Signature of Authorized TGRA Official	Signature of Authorizing NIGC Official (NIGC CJIS Systems Officer)
_____	_____
Date	Date

_____

Name of TGRA's LASO, memorializing receipt of a copy of this MOU

Guidance Appendix: CJIS Security Policy – summary of primary requirements[1]

In the MOU, the TGRA 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 TGRA in complying with the Policy, the following summarizes its primary requirements:

1. CJIS Systems Agencies (CSA)

    a. The CSA is responsible for establishing and administering an information technology security program throughout the CSA's user community.

    b. The CSA may impose more stringent protection measures than outlined in the FBI CJIS Security Policy. Such decisions shall be documented and kept current.

    c. The NIGC is a CSA. The head of each CSA shall appoint a CSO.

2. CJIS Systems Officer (CSO)

    a. The CSO is an individual located within the CSA responsible for administering the CSA's CJIS network.

    b. Pursuant to the Bylaws of the CJIS Advisory Policy Board and Working Groups, the role of CSO shall not be outsourced.

    c. The NIGC CSA CSO can be contacted by email at CSO@nigc.gov and by telephone at (202) 632-7003.

3. CJIS Systems Agency Information Security Officer (CSA ISO)

    The CSA ISO shall:

    a. Serve as the security point of contact to the FBI CJIS Division ISO.

[1] This Guidance Appendix is just that: a guidance document to use in conjunction with the CJIS Security Policy (CSP) to facilitate compliance with the CSP.

b. Document technical compliance with the CSP with the goal of assuring the confidentiality, integrity, and availability of criminal justice information to the user community and throughout the CSA's user community.

c. Document and provide assistance for implementing security-related controls for the TGRAs and its users.

d. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

e. The NIGC CSA ISO can be contacted by email at iso@nigc.gov and by telephone at (202) 632-7003.

Commented [A10]: Added at the request of Seneca Cayuga.

4. 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.

5. 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.

b. 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.[2] 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 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.

6. 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.

7. 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

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

recovery[3] as well as tracking and documenting each incident, including user response activities.[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 the NIGC ISO (iso@nigc.gov) **within 24 hours of detection**.

8. 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:

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

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 the 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.

9. 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.

10. 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.

11. 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 the 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 **within 24 hours**, and to take necessary actions. This audit must be conducted at a minimum once a week.

g. The TGRA, along with the NIGC, may be selected for a triannual audit by the FBI CJIS staff.[5]

[5] Policy sections 5.11.1.1 and 5.4.6.

Commented [A11]: Chickasaw Nation – Requiring alerts to the LASO is more stringent than the CJIS Security policy, because the CSP only requires "appropriate agency officials," which can account for users that have been classified by the TGRA as "authorized personnel" with access to the TGRA's information system.

Response – Using the term "LASO" is not more stringent and is not unnecessarily onerous. CSP 5.4.2 requires "the agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure." CSP 3.2.9 states each LASO shall "ensure the approved and appropriate security measures are in place and working as expected" and "support policy compliance and ensure the CSA ISO is promptly informed of security incidents." Consequently, the LASO is the appropriate official involved in the resolution of all audit processing failures.

12. 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 ensure these checks are performed. Please note that not all states require it and not all tribes have legal means to obtain it.[6]

13. Identification and Authentication –

    a. The TGRA shall ensure access to systems and networks used to process, store, or transmit CJI/CHRI and 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.

14. 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.

[6] Policy section 5.12.

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

    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.

16. 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.

17. Dissemination Log —

a. The TGRA shall document each release of a criminal history record, CJI, or CHRI in a dissemination log in accordance with CSP section 5.1.1.3, 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?).
    vii. How the information was disseminated (email, fax, certified mail, etc.).

18. Formal Sanctions Process

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