November 13, 2020

Dear Tribal Gaming Regulator,

The National Indian Gaming Commission (NIGC) would like to inform you of proposed changes to the Memorandum of Understanding (MOU) related to Federal Bureau of Investigation (FBI) criminal history record information (CHRI). The MOU has been revised to clearly set forth both the NIGC's and Tribes' obligations under federal law, regulations, and policies. Although the majority of these requirements are not new, both the FBI and the NIGC agree that explicitly stating them in the MOU will assist in achieving compliance. In fact, over the past year, the NIGC has been providing training and technical assistance on many of the proposed MOU mandates that derive from the federal law and regulations related to FBI CHRI and the CJIS Security Policy.

Your feedback on the draft amendments is requested so that the MOU may be implemented in a manner that causes minimal disruption and/or expense to Tribes. In providing input, please consider that NIGC is unable to modify federal law or regulations related to FBI CHRI[1] or CJIS Security Policy obligations. Please submit your comments and suggestions by December 16, 2020 to NIGC.Outreach@NIGC.gov .

Legal authority to obtain CHRI

The Indian Gaming Regulatory Act (IGRA) established federal standards for gaming on Indian lands to protect Indian gaming as a means of generating tribal revenue.[2] To carry out this purpose, Congress generally authorized the NIGC Commission to "conduct or cause to be conducted such background investigations as may be necessary" and to "promulgate regulations and guidelines as it deems appropriate to implement the provisions of" the IGRA.[3] To assist in that role, Congress specifically provided the Commission with the power to "secure from any

[1] *See, e.g.*, 34 U.S.C. § 40316; 28 C.F.R. §§16.34, 50.12(b), 901.1, 901.4(d) & 906.2.
[2] 25 U.S.C. § 2702(3).
[3] *Id.* § 2706(b)(3), (10).

department or agency of the United States information necessary to enable it to carry out" those functions.[4]

The NIGC submits fingerprints of key employees (KE) and primary management officials (PMO) of Indian gaming enterprises as part of the background screening process required by IGRA.[5] The authority to receive CHRI for KE and PMO of class II and class III gaming enterprises stems from statutory language specifically empowering the Commission to "consult with appropriate law enforcement officials concerning gaming licenses issued by an Indian tribe" and to facilitate the suspension of gaming licenses when a KE or PMO does not meet the statute's suitability and eligibility standards with regard to an applicant's criminal history.[6] Likewise, IGRA § 2711(e) requires the Chairman to review the criminal history information of persons with a direct or indirect financial interest in management contracts and to disapprove a management contract when one of those individuals "has been or subsequently is convicted of any felony or gaming offense" or where their "criminal record if any ... pose[s] a threat to the public interest or to the effective regulation and control of gaming." This, likewise, applies to both class II and class III gaming.[7]

Proposed MOU

In order for NIGC to carry out the duties and functions outlined above, the agency, through an executed MOU with FBI, will obtain CHRI from the FBI and disseminate it to the Tribes' gaming regulatory authorities (TGRA) to determine the eligibility of applicants for KE or PMO positions in the Tribes' gaming operations and enterprises.

On occasion, the NIGC updates its MOU with Tribes to include new or updated requirements and responsibilities. Attached is a proposed MOU which sets forth the responsibilities and duties of the parties for submitting noncriminal justice fingerprints; the parties' obligations for disseminating, using, and protecting CHRI; and the FBI and NIGC's conditions of its release and reuse.

The proposed MOU contains current FBI Criminal Justice Information Services (CJIS) requirements,[8] FBI conditions that you will recognize from the 2017 MOU, and a few new obligations to address issues particular to NIGC processes. The following is a non-exhaustive list of the new requirements:

- *Updating the Tribes' operating system(s) to access the NIGC fingerprint system;*

[4] *Id*. § 2708.
[5] *See* 25 U.S.C. § 2710(b)(2)(F), (c)(l)-(2), & (d)(l)(A).
[6] 25 U.S.C. § 2710(b)(2)(F)(ii)(II), (c)(l)-(2), (d)(l)(A)(ii).
[7] *See* 25 U.S.C. § 2711(e)(l)(B) & (D); 25 C.F.R. § 533.6(b)(l)(ii) & (v), (c).
[8] CJIS Security Policy v5-9 (June 1, 2020), https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view

- *Limiting fingerprinting of KEs and PMOs to those defined in NIGC regulations, 25 C.F.R. §§ 502.14(a) – (c) and 502.19(a) – (c), and not for any other purpose;*
- *Developing and implementing policies regarding applicant rights and disseminating, using, reusing, protecting and destroying CHRI;*
- *Adding the job title or position of the KE or PMO to their Notice of Results;*
- *Employing a formal sanctions process for personnel that fail to comply with information security policies and procedures; and*
- *Designating a Local Area Security Officer (LASO), who will review the MOU within 5 business days of assuming the position.*

Several of these requirements may be familiar as they are required by FBI or its CJIS Security Policy. The NIGC has spent the last year providing training on such requirements and a multitude of resources are available at https://www.nigc.gov/compliance/CJIS-Training-Materials. Please contact your Region Office or the NIGC Training Manager via email at traininginfo@nigc.gov if you need more information regarding technical assistance and training.

As noted above, please review the attached MOU[9] and provide any comments or suggestions to NIGC.Outreach@NIGC.gov by December 16, 2020. All comments and suggestions will be considered when finalizing the MOU.

Should you have questions or need further assistance, please do not hesitate to contact me at Jun_Kim@nigc.gov.

Sincerely,

Jun M. Kim Digitally signed by Jun M. Kim Date: 2020.11.13 09:32:14 -05'00'

Jun M. Kim

Chief Information Officer

CJIS Systems Officer

[9] The attached MOU has been color coded to assist the reader in the review process.

Updated 11/3/20

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 tribe] (Tribe) 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 the agreed-upon responsibilities and functions of the parties for submitting noncriminal justice fingerprints; disseminating, using, and protecting CHRI; and the FBI and NIGC's conditions of its release and reuse.

II. Parties

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

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.

B. CHRI

CHRI is a subset of CJI. CHRI means information collected by criminal justice agencies about individuals, consisting of identifiably descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. CHRI also includes information that is transferred or reproduced directly from CHRI or information that confirms the existence or nonexistence of CHRI. CHRI includes any media that contains it, such as: letters, emails, documents, notes, conversations – in person or via phone/text, and spreadsheets or tables. Examples of CHRI potentially include notice of results (NORs), licensing objection letters, and other summaries of CHRI.

IV. Authorities

The NIGC and the Tribe enter into this MOU under the NIGC's fingerprint collection/ background check authorities for class II and class III gaming enterprises that include the following: 25 U.S.C. §§ 2706(b)(3), 2706(b)(7), 2706(b)(10), 2708, 2710(b)(2)(F), 2710(c)(1)-(2), 2710(d)(9), 2711(a), 2711(e), and 28 U.S.C. § 534. Tribes are permitted to submit fingerprints to the FBI through the NIGC to obtain and use CHRI if they have an executed MOU with the NIGC.

V. Responsibilities

A. The NIGC agrees to:

1. Ensure that all fingerprint submissions have been properly and adequately completed.

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

3. Collect and remit the FBI's fee for the processing of the applicant fingerprint submission.[1]

4. Provide the Tribe with a monthly accounting and assessment of fingerprint fees due.

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

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

8. Provide timely information on all aspects of the CJIS Security Policy (Policy), the National Identity System information, and other related programs by means of technical and operational updates, newsletters, and other documents;

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

10. Audit 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.[2]

B. The Tribe:

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.

---

[1] *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).

[2] CJIS Security Policy (Policy) section 5.11.

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. Agrees to modify its operating systems to NIGC's specifications and timeframes. 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. Agrees to and understands that until federal law is amended, fingerprints of TGRA staff and/or Commissioners cannot be submitted unless the TGRA staff and/or Commissioners are key employees of the gaming operation.

7. Agrees to 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.

8. Agrees to promptly notify NIGC if the TGRA staff or Tribe become aware of any inaccuracies in PII or fingerprint data received from the NIGC.

9. Agrees that prior to taking an applicant's fingerprints, the Tribe 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, 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.[3]

[3] Written notification includes electronic notification, but excludes oral notification.

10. Agrees that if an applicant has a FBI criminal history record, the Tribe will have written policies and procedures in place to, at minimum, provide the applicant an opportunity to complete or challenge the accuracy of the information in the 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[4];

    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).

11. 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.

[4] *See* 28 C.F.R. § 50.12(b).

12. Agrees to not duplicate, disseminate, or reuse CHRI, including sharing it with applicant's spouse, household, other family members, tribal leadership, tribal agencies not involved in employing or licensing key employees or primary management officials, 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 from NIGC cannot be used for such purpose – a new record request to the FBI through a non-NIGC process must be made in such instance.

13. Agrees to 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. And agrees to establish controls to reasonably prevent unauthorized CHRI disclosure.

14. Agrees that, except in connection with proceedings related to the Tribe's licensing determinations for its key employees and primary management officials, 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(c) and 13 above or for purposes of a ke or pmo applicant's licensing or employment appeal hearing.

15. 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:

    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.).

16. Agrees to provide on the Notice of Results (NOR), the job title or position of the key employee or primary management official.

17. Agrees to grant NIGC representatives complete access to CHRI pertaining to kes and pmos. Self-regulation tribes 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. Finally, all tribes agree 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 to fully cooperate with such audits.

18. Agrees to notify NIGC of all licensing information associated with the dissemination of CHRI, such as when the NIGC has not received a NOR for an permanent employee (employed more than 90 days) whose fingerprints were submitted to the NIGC for a CHRI.

19. Agrees to comply with the FBI CJIS Security Policy (Policy), found at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center . An appendix attached to this MOU outlines the primary requirements of the Policy.

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

21. Agrees that if and when the Tribe's Local Agency Security Officer (LASO) changes, the new LASO will review a copy of this MOU within five 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

This agreement shall be effective when executed by both Parties and will continue in effect until terminated. To be clear, this agreement remains in effect regardless of personnel changes to the Parties' signatories below. This agreement may be modified at any time by written consent of both Parties.

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. CHRI dissemination to the Tribe

will cease upon suspension of services. NIGC will provide written notice of such suspension to the Tribe 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, in NIGC's discretion, the circumstances warrant immediate suspension.

Also, this MOU may be terminated with respect to any Party, at any time, upon written notice of withdrawal to the other Party. Any Party desiring to terminate or modify this MOU will provide such written notification to the other Party at least thirty (30) days prior to modification or termination. In the event of such termination, the following rules apply:

1. The parties will continue participation, financial or otherwise, through the effective date of termination;
2. All information and rights therein received under the provisions of this agreement prior to the termination will be retained by the parties, subject to the provisions of this agreement; and
3. CHRI dissemination to the Tribe will cease on or before the date of termination.

VII. Tribal Acknowledgment

The Tribe 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 to suspension of services and that failure to comply with the requirements may result in termination of services.

_____ and National Indian Gaming Commission

Name of Tribe

_____ _____

Name of Authorized Tribal Official (PRINT) Name of Authorized NIGC Official (PRINT)

_____ _____

Signature of Authorized Tribal Official Signature of Authorizing NIGC Official (NIGC CJIS Systems Officer)

_____

Name of Authorized TGRA Official, memorializing receipt of a copy of this MOU

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

[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 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.