Draft NIGC CHRI MOU: Summary of Comments

The National Indian Gaming Commission (NIGC) recently completed its initial phase of Commission Outreach on its Criminal History Record Information MOU (CHRI MOU) with Tribes and tribal gaming regulatory agencies (TGRAs). The outreach occurred from November 12 through December 16, 2020. During this time period, the NIGC invited Tribes and TGRAs to review the draft CHRI MOU and provide comments and suggestions so that the final CHRI MOU may be implemented in a manner that causes minimal disruption and/or expense to Tribes and TGRAs. Initiation of the first phase of outreach began with NIGC posting, on its website's homepage, the draft CHRI MOU and a video explaining the proposed changes to it. The next day, a letter was sent to TGRAs enclosing the draft CHRI MOU and requesting feedback. And as part of the Criminal Justice Information Services (CJIS) Symposium, a one-hour panel discussion provided an overview of the proposed changes to the CHRI MOU and responded to audience questions. The symposium was open to tribal leadership, gaming regulators and operations personnel, with 615 representatives from 195 tribes participating in the draft CHRI MOU session. Moreover, the draft CHRI MOU, explanatory video, letter, and existing 2017 CHRI MOU were all posted and accessible on the CJIS Training page of NIGC's website.

Eleven tribes submitted comments via letter or email, submitting general and specific suggestions. The majority of the Tribes and TGRA's comments were accepted in whole or in part. Input from tribal leaders and officials was also received by the NIGC during its one-hour panel discussion on the draft CHRI MOU. A summary of these comments and NIGC's responses is as follows:

CHRI MOU Parties

Submitters suggested that the MOU parties should be the NIGC and TGRAs, instead of Tribes. The change was made.

Criminal Justice Information (CJI) definition

One submission suggested that the definition of Criminal Justice Information (CJI) be altered. This suggestion was not accepted as the definition is quoted from the FBI's CJIS Security Policy (CSP).

MOU's Authority section

Another submitter suggested that the MOU's Authority section be revised to reflect NIGC's legal authority to enter the MOU as well as the specific legal authority of each Tribe to do the same. In regard to the NIGC's legal authority, this suggestion was accepted. Because it would be overly cumbersome to detail each Tribe's legal authority and because the MOU is now entered into by TGRAs, the section now reads that "TGRAs are arms of sovereign tribal governments and enter this MOU in that capacity."

Incorporation of Federal requirements

Two submitters requested that the MOU clearly incorporate federal requirements instead of summarizing them. The suggestion was accepted in part; in some instances, a summary explanation remains to assist compliance by summarizing the obligation of the requirement as well. Additionally, as a result of the FBI's audit of the NIGC, the NIGC promised that it would clarify the CHRI reuse standard in its new MOU with TGRAs.

Fingerprint processing for 25 C.F.R. § 502.14(a)-(c) and 25 C.F.R. § 502.19(a)-(c)

Several submitters recommended that if the FBI and the NIGC have agreed on certain legal interpretations that such agreement should not be imposed on Tribes or TGRAs. This suggestion was accepted by moving a provision from the TGRA section to the NIGC section of the MOU.

The same submission also was concerned that the MOU does not cover fingerprint processing for 25 C.F.R. § 502.14(d) and 25 C.F.R. § 502.19(d). Because the FBI only accepts fingerprints from the NIGC for sub-sections (a)-(c) of each provision — and incorporated this limitation in its MOU with NIGC, sub-section (d) fingerprints cannot be processed through NIGC at this time. Nothing prevents Tribes from obtaining CHRI for that purpose elsewhere, beyond the NIGC.

CJIS Security Policy compliance

One submitter requested that the NIGC "[e]nsure that submission methodology … be compliant with the FBI's CJIS Security Policy requirements" and that the NIGC "[m]aintain a log of transactions and disseminations." This suggestion was accepted in substance with the NIGC agreeing to comply with the CSP.

The same submitter proposed that the NIGC remove several provisions because they were simply a restatement of the TGRAs' agreement to abide by the CSP. Since the obligations set forth in all but one of the provisions do not derive from the CJIS Security Policy, the NIGC accepted the proposed change as to the provision derived from the CSP and rejected it as to the others.

Additional NIGC obligations

New NIGC obligations were suggested: 1) to disseminate CHRI to the authorized TGRA representative and 2) to designate a point of contact for issues and concerns related to this MOU. The MOU was changed so that NIGC will disseminate CHRI to authorized TGRA representatives and the NIGC point-of-contact provision was added.

CHRI summary memoranda

One submitter requested that NIGC remove language allowing it to furnish summary memoranda that contains solely CHRI results, because the submitter does not want to receive such from the NIGC. The change was made.

FBI-NIGC MOU provisions

A submitter requested that the NIGC agree to report to each TGRA when their information is used, disclosed or accessed in an unauthorized manner, including information losses or breaches. The submitter contends that because the NIGC has agreed to do that for CHRI in its FBI-NIGC MOU, it should do it in this MOU. This suggestion was not accepted. TGRAs do not produce CHRI, only the FBI does. Therefore, the NIGC— and accordingly the TGRAs (as related agencies) — must inform FBI when FBI's CHRI is accessed in an unauthorized manner.

The same submitter advocated that NIGC should inform TGRAs when it becomes aware of inaccuracies in information received from the TGRA, as NIGC has committed to provide the FBI the same in the FBI-NIGC MOU. The suggestion was accepted and the revised provision now obligates each Party to inform the other of inaccuracies, exactly the same as in the FBI-NIGC MOU.

Monthly Fingerprint fees

One submitter suggested that NIGC commit to providing the monthly accounting and assessment of fingerprint fees by a date certain every month. This suggestion was accepted.

Unannounced NIGC Audits

Unannounced CHRI MOU compliance audits are a concern for one submitter, who requested procedures for them and a clear definition of them. NIGC believes that CHRI MOU compliance may be achieved from announced audits and, therefore, has removed the provision for unannounced audits.

FBI rights, approvals, and restrictions

Several submitters took issue with three draft provisions that outlined the FBI's future ability to approve CHRI dissemination and impose additional restrictions. Specifically, the submitters contend that these provisions hold them to unknown standards that the FBI may apply at any time. Because these three provisions derived from NIGC's former 2017 CHRI MOU, are not required by the current FBI-NIGC MOU, and, if necessary, may be addressed with future amendments to this MOU, they were removed. However, other provisions were clarified to ensure that TGRAs abide by FBI updates to the CSP, the Next Generation Identification Audit Noncriminal Justice Access to CHRI Policy Reference Guide (NGI), and its Privacy Act Statement and Notice.

NIGC specifications for Fingerprint operating systems

Two submitters proposed that TGRAs who process their fingerprints by hard card submissions be exempt from the NIGC's specifications for fingerprint operating systems. The proposal was accepted.

Several submitters asserted that this provision was vague and required revision to plainly state

the instructions, specifications, and timeframes for the specifications. And one submitter recommended that the provision be deleted due to its vagueness and the lack of NIGC authority to require such specifications. This provision was accepted and now requires that TGRAs modify their operating systems to meet CSP and NIGC's connectivity requirements. Also, the provision provides a process for exceptions to be submitted to the NIGC ISO for approval prior to their implementation. Because technology often changes, any further specification may require cumbersome amendments to this MOU and, therefore, was not included.

TGRA Commission / Staff fingerprints

Two submitters suggested a wording change in the provision. Another urged that the provision be removed because TGRAs recognize that their commissioners and staff are not key employees of the gaming operation. Yet another contended that failing to do background investigations of TGRA personnel introduces risks to the integrity of gaming and contravenes the NIGC's legitimate law enforcement authority and its statutory basis for doing such backgrounds. In response to an FBI audit of NIGC, the NIGC agreed to instruct TGRAs that their personnel's fingerprints cannot be processed through the NIGC at this time. Because NIGC agrees that TGRAs are well aware of its instruction, the provision has been removed.

NOR addition of job title or position

One submitter asked that the NIGC clarify the basis for the provision. The NIGC did so, outlining why a job title or position is needed on NOR submissions.

NIGC access to CHRI

Two submitters suggested that the NIGC revise the provision addressing the NIGC's access to CHRI in TGRAs' possession to mirror the language in the FBI-NIGC MOU. NIGC accepted this suggestion, revising the language to afford it access to CHRI that was obtained through this MOU for purposes of inspection or audit to ensure compliance with the MOU. To be clear, if the CHRI no longer exists, the NIGC does not need access to it.

NIGC access to background & licensing files

A draft MOU provision spoke to the NIGC's access to background and licensing files for Class II and III gaming as well as to self-regulation tribes' files. Several submitters questioned why the provision was needed. Because the NIGC's access is already set forth in NIGC regulations, the majority of this provision was deleted, leaving only a provision that speaks to self-regulation tribes.

Notify NIGC of all licensing information

A draft MOU provision required that TGRAs notify the NIGC of all licensing information associated with the dissemination of CHRI. Two submitters found the characterization of "all licensing information" to be vague and overbroad. In response, the NIGC narrowed the provision to request specific licensing information connected with CHRI dissemination.

New LASOs required to review this MOU

Two submitters asked that the 5-day deadline for new LASOs to review this MOU and provide their name and contact information to the NIGC Information Security Officer (ISO) be extended to 10-days or two weeks. The suggestion for a 10-business day deadline was accepted.

Dispute Resolution provision

Several submitters recommended that a dispute resolution provision be added to this MOU for different reasons. One suggested the addition was necessary because many of the provisions and standards in the MOU are ambiguous. Since the vast majority of tribal comments were accepted, the provisions and standards have been clarified in line with tribal suggestions. Others recommended that informal government-to-government discourse should occur first. A dispute resolution provision is unnecessary because in most instances a TGRA will receive a 30-day notice of suspension and a detailed description of the issues to correct prior to the suspension occurring. Additionally, if requested, TGRAs will be afforded another 30-day period to respond or correct issues associated with a suspension notice or submit a written plan of action in a timeframe acceptable to both Parties. The only exception is a situation of imminent risk, which is defined in the agreement. In addition, termination also requires a 30-day notice and CHRI will still be distributed unless there is imminent risk.

Effective date and period of MOU

One submitter suggested specific language concerning the effective date and period of the MOU. Such language was accepted in part. Because there is a separate provision in the MOU addressing termination, the suggested language addressing it was not accepted.

MOU Modifications

The same submitter suggested specific language regarding how modifications to the MOU are made and the effective date of them. These suggestions were accepted in substance.

Another submitter recommended an annual term period to allow for revisions and updates due to changes in law. This recommendation was not adopted because changes in law will come under the modification provision of the MOU, requiring the NIGC to provide TGRAs 30-days' notice of them and the need to update the MOU.

Suspension of Services under the MOU

Two submitters pointed out that suspension of services due to a potential breach of any MOU term was overly vague and ambiguous. The term "potential" was removed.

One submitter requests not only 30-days' prior notice of suspension but also an additional 30-days to remedy the issues that are the grounds for the suspension. The suggestion was accepted.

Termination of Services under the MOU

A submitter suggested that new grounds for terminating services under the MOU, such as repeated failure to adhere to the CSP, repeated disregard for federal laws, and substantial breach of the MOU. This suggestion was not accepted, as the NIGC believes that the processes and timelines set forth in both the suspension and termination provisions are fair. Specifically, suspension affords a 30-day notice and potentially 30-days to respond or remedy the breach or to submit a plan of action that corrects the breach within a timeframe agreed upon by the Parties. Termination also affords 30-days' notice. And in both cases, services are not suspended unless there is imminent risk.

Two submitters contend that access to CHRI is critical and therefore should only be terminated for violation of the MOU or federal requirements. The NIGC agreed and modified the provision accordingly.

Another submitter stated that services should only cease on the date of termination, meaning after NIGC provides 30-days' written notice. The NIGC accepted this suggestion in part, revising the provision so that services will cease on the date of termination unless suspended prior to such date due to the existence of imminent risk. Imminent risk is now defined in the MOU.

Tribal Acknowledgment section

A submitter asserted that there were no grounds for including a tribal acknowledgment in the MOU. Because the acknowledgment was duplicative of other provisions in the MOU, it has been deleted.

General comments

Allow compliance flexibility where possible

The NIGC has attempted to do this in its Revised draft CHRI MOU.

Limit the MOU's application to the NIGC's/TGRA's obligations

The NIGC has requested additional requirements or information in only three instances, each to ensure CHRI compliance. (i.e. fingerprint operating systems, job title on NORs, and explanation of non-submission of NORs). Also, as to self-regulation tribes, NIGC requires access to Class II background investigation and licensing files for purposes of confirming compliance.

The MOU is a one-size fits all MOU, applying to all Tribes instead of recognizing the difference in operating systems and types of gaming offered by each. And the MOU's requirements and restrictions are unnecessary and punitive.

The federal requirements for CHRI are one-size fits all, with the exception of outsourcing agreements, which are dependent upon individual circumstances. Further, the type of gaming

offered does not impact CHRI requirements. The MOU outlines the federal requirements that are mandatory. As explained above, NIGC has only requested additional information in two instances and requirements as to operating systems. All of which is necessary to ensure CHRI compliance. Because the modification, suspension, and termination provisions all include 30-day notice periods (unless imminent risk exists) and other reasonable processes, they are not punitive.

The MOU includes every single FBI policy and procedure and NIGC did not agree to such in the FBI-NIGC MOU.

The NIGC also signed a User Agreement with the FBI that incorporates such policies and procedures as well as federal law and regulation, requiring compliance.