Ensuring the Integrity of Criminal Justice Information

by Dave Vialpando

The risks to the integrity of casino gaming and the protection of tribal assets require Tribal Gaming Regulatory Agencies (TGRAs) to thoroughly vet those who work in tribal casinos. An integral part of this vetting process conducted by TGRA licensing personnel across the country is an analysis of the criminal history records of tribal gaming key employees and primary management officials.

An essential resource in accessing a gaming license applicant's Criminal Justice Information (CJI) or Criminal History Record Information (CHRI) is the National Indian Gaming Commission (NIGC) which has established an agreement with the Federal Bureau of Investigation (FBI) to serve as a conduit for TGRAs to access CHRI maintained by the FBI, based on applicant automated or manual fingerprint submissions. The FBI and the NIGC are currently ensuring that TGRAs are exercising the required level of care in the handling, processing, and storage of CHRI with the NIGC conducting CJI/CHRI audits of TGRAs across the country and the FBI planning to visit a few TGRAs in 2021 and 2022 to ensure regulatory compliance.

The FBI serves as a central repository or conduit for CHRI provided by a majority of criminal justice agencies across the U.S. Not all law enforcement agencies provide their CHRI to the FBI, but a significant number of them do to the point that a CHRI query of the FBI through the NIGC can provide valuable information to TGRAs regarding possible criminal histories of gaming license applicants and their corresponding level of risk to the gaming operation.

The dissemination and processing of CHRI is highly regulated by the FBI, and misuse or mishandling of a person's CHRI may result in significant sanction and a prohibition on a TGRA accessing this valuable information from the FBI in the future. A TGRA must meet a wide spectrum of regulatory requirements enforced by the NIGC in order to process a license applicant's fingerprints for CHRI. Some state gaming agencies cannot meet the stringent federal regulatory requirements enforced by the FBI. Recently, the FBI denied a request by the Michigan Gaming Control Board to process automated fingerprints for state gaming licenses until federal requirements are met.

It is important to note that the NIGC has established extensive training and resource guides to assist TGRAs in ensuring regulatory compliance related to CHRI. To clarify further, CHRI is any information collected by criminal justice agencies on individuals consisting of identifying information and information concerning arrests, detentions, indictments, information, or other formal criminal charges, any disposition arising from these actions, including acquittal, sentencing, correctional supervision (probation or parole), and release. In 1993, the NIGC established a Memorandum of Understanding (MOU) with the FBI for the dissemination of CHRI to qualifying TGRAs as provided for in the Indian Gaming Regulatory Act (IGRA) and NIGC regulations. The NIGC processes fingerprints of key employees and primary management officials submitted by TGRAs and provides TGRAs with CJI and CHRI obtained from the FBI for noncriminal justice purposes as authorized by federal law. It is important to note that without the NIGC's MOU with the FBI, the NIGC would not have the ability to share FBI CHRI with the tribes enabling the NIGC to carry out the agency's duties under IGRA. Without the NIGC's MOU, tribes would not be eligible under IGRA or any other current federal legislation to receive the FBI CHRI for the purpose of licensing key employees and primary management officials. There are some instances where state law may authorize the tribe to receive FBI CHRI through the state for Class III licensing or certification purposes

The framework utilized by the FBI for collecting CHRI from criminal justice agencies in the U.S. and disseminating CHRI to non-criminal justice agencies is outlined in the National Crime Prevention and Privacy Compact Act of 1998, the National Crime Prevention and Privacy Compact Council and the FBI's Criminal Justice Information Services (CJIS) Security Policy. A key component of all these documents is protection of individual privacy rights. NIGC regulations and TGRA policies and procedures regarding the management of CHRI are designed to ensure the integrity of CHRI and the protection of applicant privacy rights.

The preeminent guide for TGRAs in the management of CHRI and regulatory compliance standards is the NIGC's Noncriminal Justice Agency Guide for Federal Criminal History Checks. The first step in reviewing a TGRA's compliance with NIGC regulations is to ensure that the TGRA has a current executed MOU with the NIGC. This MOU will outline the authority and purpose of the MOU, sanctions and penalties resulting from the misuse of CHRI, designation of a Local Agency Security Officer (LASO) by the TGRA, required training of TGRA staff, and the TGRA's responsibility for developing policies and procedures providing for the security and proper handling of CJI and CHRI.

The TGRA must document that all staff subject to the MOU and accessing CHRI have reviewed the MOU. TGRAs are prohibited from disseminating CJI or CHRI to outside agencies, including other TGRAs and criminal justice agencies.

The TGRA must designate a LASO who will oversee all components of the TGRA's CHRI training, access, management, and disposition processes. The LASO must maintain a current list of TGRA authorized personnel having access to FBI CHRI and notify the NIGC of any changes in authorized personnel. The LASO is responsible for ensuring that all authorized personnel complete the CJIS Security Awareness Training and serves as the primary point of contact between the TGRA and the NIGC on matters related to CHRI management. The LASO must complete specialized training as outlined in the FBI CJIS Services Security Policy. The TGRA must retain all training records for a minimum of two years.

The next step in ensuring regulatory compliance is development of comprehensive TGRA policies and procedures covering the following areas: use of fingerprint-based CHRI (key employees and primary management officials only); Applicants Rights Notice/FBI Privacy Act Notice/ Opportunity to Correct/Copy of CHRI (a policy prohibiting dissemination of CHRI is permissible as long as applicants are provided with information on how to obtain their own copy from the FBI); Security Awareness Training; Incident Response Policy (including the TGRA's Incident Reporting Form, all incidents must be reported to the NIGC within 24 hours of detection); Auditing and Accountability (including access to CHRI, storage, destruction, and required non-channeler audits); access control, identification and authentication (confirming applicant identification, typically by an unexpired form of government-issued photo identification); current acknowledgment statements signed by those accessing CHRI (to include consequences for misuse); configuration management; media protection (many TGRAs are prohibiting storage of CHRI on external IT media); physical protection (many TGRAs are going paperless so physical storage is not an issue; off-site storage of CHRI through a third-party may require an FBI-approved non-channeler agreement); system and communication protection and information integrity; personnel security; and use of mobile devices. In short, if the TGRA has a process that involves FBI CHRI, it should be cited in an approved policy or procedure. This is helpful for both the NIGC audit process and training employees new to the CJIS process.

An excellent template for TGRA policy and procedure development can be found in Appendix F of the NIGC Noncriminal Justice Agency Guide for Federal Criminal History Checks. In fact, the Appendix section of this document contains samples of many of the required forms and documents, such as privacy notices, which can be modified for TGRA use. Although not required by regulation, in certain areas of the country, the TGRA might consider developing a Spanish version of the required privacy notices.

TGRAs must evaluate the need to establish Outsourcing Agreements for non-channelers (companies or services outside of the TGRA). Examples of entities that may require outsourcing agreements include IT service providers, physical storage facilities, shredding services, and automated fingerprint equipment suppliers. In determining the need for an outsourcing agreement, the TGRA should track FBI CHRI or summary FBI CHRI throughout its lifespan with the TGRA and determine who has or will have access to the information at any point in time. An entity outside of the TGRA who has or will have access to CHRI will probably require an outsourcing agreement.

If an outsourcing agreement is required a request letter and unexecuted outsourcing agreement must be sent by the TGRA to the FBI Compact Officer for outsourcing contract approval. Once approved, a non-channeler agreement is established between the TGRA and the service provider. The TGRA must conduct an audit on the contractor within 90-days from the execution of the agreement. (Templates for the request letter to the FBI, non-channeler agreement, and audit checklist can be found in The Outsourcing of Noncriminal Justice Administrative Functions Guide for Federal Agencies.) To ensure quick approval of the agreement, be sure to specify exactly what service the contractor will perform and/or how they will have access or potential access to the FBI CHRI. The templates list very broad examples to help TGRA's identify what services are anticipated.

CHRI management by the TGRA is a continual process with required documented audits, monitoring and recurrent training for users and outsourced non-channelers for the duration of the TGRA's MOU with the NIGC for access to FBI CJI and CHRI. TGRAs should consider the fact that once the CHRI has served its purpose in assisting in the determination of suitability for licensing, unless retention is required by TGRA policy, retention may not be necessary and consider purging this data. The fewer the number of retained CHRI records, the lower the risk of mishandling or compromise. It is important to know the actual FBI CHRI results received from the NIGC is not one of the items listed to be retained in 25 CFR Parts 556 or 558. The actual fingerprints are required to be retained, but not the CHRI results. TGRAs should be aware that the notice of results and the investigative report likely contains summary FBI CHRI

"The audit process, as experienced by the Pokagon Band Gaming Commission, has been professional and collaborative."

and investigative reports, which are required to be retained for three years post termination of employment

NIGC staff are currently conducting CHRI audits of TGRAs across the country. According to Meredith Hanley, Director of Licensing and Investigations and LASO for the Pokagon Band Gaming Commission, "The audit process may appear daunting at first, however utilization of NIGC appendices, checklists and forms will guide your TGRA through the process. The NIGC audit is designed to ensure all TGRA keep CHRI safely within FBI parameters and should not be seen or approached as punitive." According to Tom Cunningham, Acting Director of Compliance for the NIGC, " The protection of FBI CHRI and compliance with the CJIS policies is a shared responsibility. NIGC will continue to work hand in hand with the TGRAs and the FBI CJIS Audit Unit to achieve these goals."

The audit process, as experienced by the Pokagon Band Gaming Commission, has been professional and collaborative. Reviewing the CHRI Audit Checklist ahead of time, gathering the required policies, procedures, TGRA audit results, and documentation prior to the NIGC audit, and remaining receptive to the suggestions and input of the experienced NIGC auditors is not only likely to result in an audit free of findings, but will ensure that all of the appropriate components are in place to ensure the integrity of CJI/CHRI and protection of the privacy rights of our gaming industry employees. ♣

David Vialpando is Executive Director of the Pokagon Band Gaming Commission. He can be reached by calling (269) 926-5485 or email david.vialpando@pokagonband-nsn.gov.