National Indian Gaming Commission
Privacy Impact Assessment – NIGC-GSS
(NIGC PIA Form)

Introduction

The NIGC requires Privacy Impact Assessments (PIA) to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically.

System: National Indian Gaming Commission-General Support System (NIGC-GSS)

Date: October 26, 2023

Agency: National Indian Gaming Commission

Office: Office of Chief Information Officer (Division of Technology)

Point of Contact:

Email:milton.cartwright@nigc.gov
First Name: Milton
Last Name: Cartwright Jr
Phone: 202.632.7003
Address Line 1: 90 K St., Suite 200
Address Line 2:
City: Washington
State/Territory: DC
Zip: 20002

Section 1. General System Information

A. Is a full PIA required?

This is a threshold question. Indicate whether the system collects, maintains, uses or disseminates information about members of the general public, Federal employees, or contractors. If the system does not contain any information that is identifiable to individual (e.g., statistical, geographic, financial), complete all questions in this section and obtain approval and required signatures in Section 5. The entire PIA must be completed for systems that contain information identifiable to individuals, including employees, contractors and volunteers.

NIGC PIA Form

☒ Yes, information is collected from or maintained on

☒ Members of the general public

☒ Federal personnel and/or Federal contractors

☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

Describe the purpose of the system and how it relates to the program office's and Commission's mission. Include the context and background necessary to understand the purpose, the name of the program office and the technology, project or collection being assessed.

The Indian Gaming Regulatory Act (IGRA or the Act), Public Law 100–497, 25 U.S.C. 2701, *et seq.*, was signed into law on October 17, 1988. The Act crafted a framework for the regulation of gaming on Indian lands and established the National Indian Gaming Commission (NIGC or Commission) as the Federal regulatory authority responsible for the implementation of IGRA. Commission regulations include: reviews and approvals of Tribal gaming ordinances and gaming management contracts; training on, and where necessary the enforcement of, requirements of the IGRA; and, in general, providing support to Tribal gaming regulatory authorities.

The NIGC-GSS securely stores and manages all Commission information assets, provides network connectivity to eight regional offices, and delivers core applications and services to both internal and external stakeholders. It is the fundamental component of the NIGC's IT infrastructure and essential for the NIGC's fulfillment of its mission under the IGRA.

C. What is the legal authority?

A Federal law, Executive Order of the President (EO), or NIGC requirement must authorize the collection and maintenance of a system of records. For Privacy Act systems, the response should reflect the information provided in the authority section of the Privacy Act system of records notice.

44 U.S.C. 3101, *et seq.*

25 U.S.C. 2701, *et seq.*

25 CFR part 501 *et seq.*

D. Why is this PIA being completed or modified?

Indicate why the PIA is being conducted. For example, the system is being significantly modified or two systems are being merged together.

☐ New Information System
☐ New Electronic Collection
☒ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Enter "None" if no subsystems or applications are hosted. For General Support Systems (GSS) be sure to include all hosted major applications, minor applications, or other subsystems, and describe the purposes and types of PII if any. Privacy risks must be identified and adequately addressed for each hosted application or subsystem identified in the GSS PIA.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Tribal Information Management System (TIMS)	Handles the submission, processing, and results of FBI fingerprint background checks conducted as part of Tribal gaming licensing process.	Yes	Fingerprint cards and associated card information, criminal history record information, tribal licensing applicant information.
Microsoft 365	Electronic file storage for provisioning across the agency divisions and programs. Also includes associated licensed applications (email, collaborative workspaces etc.)	Yes	Tribal gaming employee licensing information located in Compliance files. NIGC employee HR-related information located in HR files. NIGC employee EEO-related information located in EEO files. Names and personal information that may be located in Compliance investigative files. Names and individual training participation information that

			may be located in Training files. Names and personal information that may be located in Office of General Counsel enforcement, lands and/or general law files.
Sumo Logic	Administrative tool for centralized monitoring of system and system logs	No	
Zoom Gov	Enables virtual audio/video calls and meetings	No	
Samanage (Solarwinds)	IT (servicing) ticket system	Yes	Names of employees who report IT issues and of external partners using the Kiteworks system who seek technical assistance with the system.
Accellion Kiteworks	Secure platform for file sharing and transfers	Yes	Tribal gaming employee licensing information transmitted to/from associated Compliance files. NIGC employee HR-related information transmitted to/from HR files. NIGC employee EEO-related information transmitted to/from EEO files. Names and personal information transmitted to/from Compliance investigative files. Names and training participation information transmitted to/from Training files. Names and personal information transmitted to/from Office of General Counsel enforcement, lands and/or general law files.

F. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about individuals that is retrieved by name or other unique identifier. Provide the NIGC or Government-wide Privacy Act SORN identifier and ensure it is captured for this system. For new SORNS being developed, select "Yes" and provide a detailed explanation. Contact the NIGC Privacy Officer for assistance identifying the appropriate Privacy Act SORN(s).

☒ Yes: *List Privacy Act SORN Identifier(s)*
☐ No

Indian Gaming Individuals Record System-NIGC-1. Vol. 88, No. 46 FR 14648 March 9, 2023.

Management Contract Individuals Record System-NIGC-2. Vol. 88, No. 46 FR 14642 March 9, 2023.

Payroll, Attendance, Retirement, and Leave Records – NIGC-3. Vol. 88. Mp/ 46 FR March 9, 2023.

NIGC Reasonable Accommodations Records. Vol. 86, No. 237 FR 71090 December 4, 2021.

Government-wide SORNs, such as for HR, EEO etc., are also applicable to some sub-system collections.

G. Does this information system or electronic collection require an OMB Control Number?

The Paperwork Reduction Act requires an OMB Control Number for certain collections of information from ten or more members of the public. If information is collected from members of the public, contact the NIGC Records Officer for assistance to determine whether you need to obtain OMB approval. Please include all OMB Control Numbers and Expiration Dates that are applicable.

☒ Yes: *Describe*
☐ No

OMB IC 3141-0004, Indian Gaming Management Contract Provisions, Approved, Expiration 02/28/2026.

OMB IC 3141-0003, Class II and III/ Background Investigation Tribal Licenses, Approved, Expiration 07/31/2023 (Currently under review by OMB for renewal).

OMB IC 3141-0008, Issuance of Certificates of Self-Regulation to Tribe for Class II Gaming, Approved, Expiration 07/31/2023 (Currently under review by OMB for renewal).

OMB IC 3141-00012, Facility License Notifications and Submission, Approved, Expiration 12/31/2025.

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

Identify all the categories of PII that will be collected, stored, used, maintained or disseminated. Describe any additional categories of PII not already indicated, as well as any new information that is created (for example, an analysis or report), and describe how this is done and the purpose of that information.

☒ Name
☒ Citizenship
☒ Gender
☒ Birth Date
☒ Group Affiliation
☒ Marital Status
☒ Biometrics
☒ Other Names Used
☒ Truncated SSN
☒ Legal Status
☒ Place of Birth
☒ Religious Preference
☒ Security Clearance
☒ Spouse Information
☒ Financial Information
☒ Medical Information
☒ Disability Information
☒ Credit Card Number
☒ Law Enforcement
☒ Education Information
☒ Emergency Contact
☒ Driver's License
☒ Race/Ethnicity
☒ Social Security Number (SSN)
☒ Personal Cell Telephone Number
☒ Tribal or Other ID Number
☒ Personal Email Address
☒ Mother's Maiden Name
☒ Home Telephone Number
☒ Child or Dependent Information
☒ Employment Information

☒ Military Status/Service
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*

Other: Place of birth, height, weight, eye color, hair color, FBI number, education, signature, current business telephone number, description of any existing and previous business relationships with Indian tribes, a description of any existing and previous business relationships with the gaming industry generally, the name and address of any licensing or regulatory agency with which a person has filed an application for a license or permit related to gaming and determination of the license (granted, denied, revoked), a photograph, resume.

B. What is the source for the PII collected? Indicate all that apply.

Include all sources of PII collected. For example, information may be collected directly from an individual through a written form, website collection, or through interviews over the phone or in person. Information may also come from agency officials and employees, agency records, from a computer readable extract from another system, or may be created within the system itself. If information is being collected through an interface with other systems, commercial data aggregators, or other agencies, list the source(s) and explain why information from sources other than the individual is required.

☒ Individual
☒ Federal agency
☒ Tribal agency
☒ Local agency
☐ NIGC records
☒ Third party source
☒ State agency
☐ Other: *Describe*

C. How will the information be collected? Indicate all that apply.

Forms completed by individuals. Documents submitted by individuals. Interviews of individuals. Documents submitted by Tribes. Documents acquired from other Federal agencies. Documents acquired from non-Federal governmental entities. Information acquired from public sources. Documents acquired by investigators.

D. By what means is the information received?

Indicate all the formats or methods for collecting PII that will be used. If the system receives information from another system, such as a transfer of financial information or

response to a background check, describe the system from which the information originates, how the information is used, and how the systems interface.

☒ Electronic File
☒ Email
☒ Face-to-Face Contact
☒ Web site
☒ Fax
☒ Telephone Interview
☒ Information Shared Between Systems (see below)
☒ Other: *Describe*

Fingerprint card images and information are electronically submitted to the FBI via the NIGC's Tribal Information Management System (TIMS). The FBI transmits results back to the TIMS where the results are made accessible to requesters. In a small portion of cases, the NIGC provides assistance by accepting physical fingerprint cards and digitizing/uploading them into the TIMS on behalf of the requester.

Tribes routinely send notices (applicant results, licensing/not licensing, licensing revocation) to the NIGC as part of the tribal licensing process. These notices are transmitted over an NIGC file-sharing system.

NIGC compliance investigators receive electronic files in response to document requests. These files are transmitted over email.

The NIGC Tribal Self-Regulation Program annually receives, via hard copy or email, the resumes of self-regulating tribal gaming regulators.

NIGC Training receives information via electronic forms and tracks registration, participation and completion of NIGC training.

NIGC HR, Accounting and Payroll shares employee information with DOI HR systems and also via email.

The Office of the General Counsel (OGC) receives information via email or secure file transfer platform.

E. What is the intended use of the PII collected?

Describe the intended uses of the PII collected and maintained in the system and provide a detailed explanation on how the data will be used. The intended uses must be relevant to the purpose of the system; for Privacy Act systems, uses must be consistent with the published system of records notice.

Tribal licensing related background investigative information is used by Tribes, in coordination with the NIGC, to perform employment applicant reviews and to ensure that Tribes have adequate information for making gaming licensing decisions.

Management contractor background investigative information is used by the NIGC to make determinations about the character and suitability of proposed gaming management contractors.

Compliance investigative information is used by the NIGC investigators to monitor tribal gaming facilities and to identify any instances in which persons may be involved in violating the IGRA.

The Office for Self-Regulation annually reviews the composition of tribal gaming regulatory authorities of self-regulating tribes as part of the NIGC's regulatory oversight function.

OGC uses facility lands information to ascertain ownership of lands as part of the formulation of Indian lands opinions and/or Indian lands compliance reviews.

Employee information pertaining to payroll, personnel, EEO, and reasonable accommodation matters is used to properly administer the staffing of the NIGC.

Training program information is used to create reports to track training participation, perform quality control and maintain program accountability.

F. With whom will the PII be shared, both within NIGC and outside NIGC? Indicate all that apply.

Indicate all the parties, both internal and external to NIGC, with whom PII will be shared. Identify other NIGC offices with assigned roles and responsibilities within the system, or with whom information is shared, and describe how and why information is shared. Also, identify other federal, state and local government agencies, private sector entities, contractors or other external third parties with whom information is shared; and describe any routine information sharing conducted with these external agencies or parties, and how such external sharing is compatible with the original purpose of the collection of the information. If sharing is pursuant to a Computer Matching Agreement, provide an explanation. For Privacy Act systems, describe how an accounting for the disclosure is maintained.

Background investigative licensing is shared in accordance with routine uses detailed in the System of Records Notice published as: Indian Gaming Individuals Record System-NIGC-1. Vol. 88, No. 46 FR 14648 March 9, 2023.

Management contract background investigative information is shared in accordance with routine uses detailed in the System of Records Notice published as: Management Contract Individuals Record System-NIGC-2. Vol. 88, No. 46 FR 14642 March 9, 2023.

HR and payroll information is shared in accordance with routine uses detailed in the System of Records Notice published as: Payroll, Attendance, Retirement, and Leave Records – NIGC-3. Vol. 88. Mp/ 46 FR March 9, 2023.

Reasonable Accommodation information is shared in accordance with routine uses detailed in the System of Records Notice published as NIGC Reasonable Accommodations Records. Vol. 86, No. 237 FR 71090 December 4, 202.

Compliance investigative information is shared internally with the OGC for providing legal counsel and with NIGC leadership for decision-making.

Self-regulation information is not routinely shared outside of the Self-Regulation program.

Training information about individuals is not routinely shared outside of the Training program.

Information acquired by the Office of the General Counsel is shared with the Commission and decision-makers as part of the OGC's role in providing legal guidance and advice to the Commission.

G. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

If "Yes," describe the method by which individuals can decline to provide information or how individuals consent to specific uses. If "No," state the reason why individuals cannot object or why individuals cannot give or withhold their consent.

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

Tribal applicant/licensing information collection forms contain a notice advising that failure to consent to the disclosures indicated in the notice will result in a tribe being unable to issue a license. The collection is required under NIGC regulations.

Tribal management contractor information collection forms contain a statement advising that failure to consent to the disclosures indicated in the statement will result in the NIGC

being unable to approve the contractor/contract. The collection is required under NIGC regulations.

NIGC HR information collection forms contain notices advising of the routine uses of the information. The collection of information is necessary for fulfilling employment and administrative functions.

Training information collection forms are provided as requested. The collection is voluntary but necessary for the administration of the training program.

H. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

Describe how notice is provided to the individual about the information collected, the right to consent to uses of the information, and the right to decline to provide information. For example, privacy notice to individuals may include Privacy Act Statements, posted Privacy Notices, privacy policy, and published SORNs and PIAs. Describe each format used and, if possible, provide a copy of the Privacy Act Statement, Privacy Notice, or a link to the applicable privacy policy, procedure, PIA or referenced SORN Federal Register citation (e.g., XX FR XXXX, Date) for review. Also describe any Privacy Act exemptions that may apply and reference the Final Rule published in the Code of Federal Regulations (43 CFR Part 2).

☒ Privacy Act Statement: *Describe each applicable format.*

☐ Privacy Notice: *Describe each applicable format.*

☐ Other: *Describe each applicable format.*

☐ None

Notice is provided by the SORNs noted above (see Section 1G) and as published in the Federal Register.

The employee administrative forms that collect HR, payroll etc. information contain privacy notices during the application and hiring process, for example, Privacy & security | Login.gov.

Tribal applicant/licensing forms contain a privacy notice as required by NIGC regulations at 25 CFR 556.2: https://www.ecfr.gov/current/title-25/section-556.2. FD-258 fingerprint cards also contain a Privacy Act statement: FD-258 Privacy Act Statement — FBI.

Tribal management contractor forms contain a privacy statement as required by NIGC regulations at 25 CFR 537.1(b)(4): https://www.ecfr.gov/current/title-25/section-537.1.

Standard Form 85P, which is a collection instrument used in this process, contains a Privacy Act statement detailing routine uses: sf85p.pdf (opm.gov)

I. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Describe how data is retrieved from the system. For example, is data retrieved manually or via reports generated automatically? Are specific retrieval identifiers used or does the system use key word searches? Be sure to list the identifiers that will be used to retrieve data (e.g., name, case number, Tribal Identification Number, subject matter, date, etc.).

For structured data, such the TIMS, information can be retrieved by filtering on fields such as individual full name, social security number, or tribal affiliation.

For unstructured data, individual information is most commonly retrieved by accessing a designated file/folder or conducting term searches.

J. Will reports be produced on individuals?

Indicate whether reports will be produced on individuals. Provide an explanation on the purpose of the reports generated, how the reports will be used, what data will be included in the reports, who the reports will be shared with, and who will have access to the reports. Many systems have features that allow reports to be generated on data in the system or on user actions within the system.

☒ Yes: *What will be the use of these reports? Who will have access to them?*
☐ No

NIGC regulations require that tribal authorities create reports for certain categories of gaming employment applicants. These individual reports summarize the findings of the tribal background investigation of tribal gaming applicants. Tribal authorities are required to consider these findings as part of their application review process. The tribes are also required to share these reports with the Commission and they are reviewed by regional compliance personnel.

Tribes routinely send notices (results, licensing/not licensing, licensing revocation) that are reports to the NIGC as part of the tribal licensing process. The notices are transmitted over a secure file transfer platform and maintained in dedicated document libraries where they can be accessed by compliance officers and regional personnel to review and monitor tribal gaming licensing.

The NIGC TIMS maintains standardized reports that are accessed by NIGC compliance personnel who monitor tribal employment application and licensing processes. These reports include summaries and details of tribal notices relating to tribal licensing

decisions and include the capability to filter information at the individual level. TIMS also maintains reports that list an individual's tribal employment history and these reports are made available to tribal background investigators to assist in verifying an individual's tribal gaming experience.

NIGC Management Contracts Background Investigators create reports on prospective gaming management personnel and entities. These reports assess the suitability of persons with a financial interest in, or management responsibility for, a tribal gaming management contract and are shared with the Chairperson as part of the NIGC's management contract review process.

NIGC Compliance Investigators create investigative reports and these reports sometimes include business and background information about individuals involved in Indian gaming. The reports are typically shared with the OGC and the Commission and information within the reports may be incorporated into an enforcement action.

NIGC HR, Payroll, EEO, and Reasonable Accommodation programs compile reports to assist in the performance of their agency administrative functions and for accountability purposes.

Section 3. Attributes of System Data

A. How will data be collected from sources other than NIGC records be verified for accuracy?

Data accuracy and reliability are important requirements in implementing the Privacy Act which requires that agencies only maintain data that is accurate, relevant, timely, and complete about individuals. The information has to have some form of verification for accuracy due to the Privacy Act provisions that require that only relevant and accurate records should be collected and maintained about individuals.

Tribal gaming applicant and management contractor background information is collected from individuals submitting forms. The forms contain a "notice regarding false statements" that serves as warnings against submitting false or inaccurate information. The information submitted is verified by an investigation which includes running FBI fingerprint background checks. Applicants are also allowed to examine and challenge the accuracy of the information that is collected from the background investigation and this is considered in the applicant decision-making process.

HR, Payroll and other employee administrative information originates in forms submitted by individuals and is verified by background investigations.

Training information is verified by checking the identity of persons at events and by email account information for online events.

B. How will data be checked for completeness?

Describe the procedures to ensure data is checked for completeness. To the extent practical, PII should be checked for completeness to ensure accuracy within the context of the use of the data.

Forms are manually and individually checked for completeness.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Describe the steps or procedures taken to ensure the data is current and not out-of-date. Where are they documented? For example, are they outlined in standard operating procedures or data models? Data that is not current also affects the relevancy and accuracy of the data. This is particularly true with data warehousing. A data warehouse is a repository of an organization's electronically stored data and is designed to facilitate reporting and analysis. A data warehouse may contain data that is not current which would cause a domino effect throughout the data stores.

Tribal gaming licensing information is collected at the start of the application process. NIGC regulations require that licensing decisions are made within 90 days of an applicant being hired. This timeline ensures that information collected for consideration in the decision-making process is current and not out-of-date.

Management contractor background information is collected at the start of the investigatory process. NIGC regulations require that the information is current. For example, business and residence telephone numbers must be "current"; descriptions of business relationships must include "existing" relationships; financial statements submitted must be for the "previous three (3) years."

HR, Payroll and other employee administrative information is regularly updated as needed.

Training information is regularly updated as needed.

NIGC regulations require that tribal self-regulation submissions be updated annually.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Identify all applicable records retention schedules or explain at what development stage the proposed records retention schedule is in. Information system owners must consult with the NIGC Records Officers early in the development process to ensure that

appropriate retention and destruction schedules are identified, or to develop a records retention schedule for the records contained in the information system. Be sure to include applicable records retention schedules for different types of information or subsets of information and describe if subsets of information are deleted and how they are deleted.

Information collections that contain PII are managed under the following NARA-approved records retention schedules:

Tribal employment and licensing information managed by IT – Tribal Background Information System under Schedule DAA-0600-2017-0011/2020-0001

- Item 2 Applicant Background Information – files cut off at the end of the calendar year, destroy 5 years after cutoff
- Item 3 Criminal History Record Information – destroy 1 year after received from the FBI

Tribal management contracts background investigative information managed by Finance – Management Contracts Reviews under Schedule DAA-0600-2017-0008

- Item 6 Background Investigations Submitted Documents and Working Files – files cut off at the end of the calendar year in which the background investigation completed, destroy 7 years after cutoff
- Item 4 Background Investigation Final Report – files cut off at the end of the calendar year in which the contract review completed or terminated, destroy 10 years after cutoff

Compliance licensing notices information is managed by Compliance – Field under Schedule DAA-0600-2017-0003

- Item 5 Tribal Notices of Results (NORs) - cut off files at end of calendar year, destroy 3 years after cutoff.
- Item 6 Tribal Notices of Issuance of a License (IOL) - cut off files at end of calendar year, destroy 3 years after cutoff. Temporary.

Tribal Gaming Investigations information is managed by Compliance – Field under Schedule DAA-0600-2017-0003

- Item 3 Tribal Gaming Investigations - cut off files at end of calendar year, destroy 3 years after cutoff.

Tribal self-regulation information managed by the Office of Chairperson and Commission under Schedule DAA-0600-2017-0001

- Item 11 Tribal Self-Regulation Application and NIGC Review Working Files - cut off files at end of calendar year, destroy 7 years after cutoff.
- Item 12 Self-Regulation Annual Submissions - cut off files at end of calendar year, destroy 7 years after cutoff.

Training participation information managed by Compliance – Training under Schedule DAA-0600-2017-0006 -

- Item 3 Tribal Training Events - Cut off files at end of calendar year. Destroy 5 years after cutoff.

Indian lands information managed by Office of the General Counsel under Schedule DAA-0600-2017-0002

- Item 12 OGC Indian Lands Database - cut off when associated land's review matter is closed, destroy no sooner than 10 years after cutoff but longer retention is authorized.

HR, payroll, EEO, reasonable accommodation and common Federal administrative records are managed under applicable general records schedules (GRS) approved and published by NARA.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Describe policies and procedures for how PII that is no longer relevant and necessary is purged. This may be obtained from records retention schedules, agency and/or records management policies, or standard operating procedures.

Tribal employment and licensing information that is highly sensitive is purged from the system on an automated monthly schedule.

Management contracts background investigative information is archived in folders and manually purged at the folder level.

Compliance licensing notices information is archived in folders and manually purged at the folder level.

Compliance investigative information is archived in folders and manually purged at the folder level.

Training participation information is archived in folders and manually purged at the folder level.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

Describe and analyze the major potential privacy risks identified and discuss the overall impact on the privacy of employees or individuals. Include a description of how the program office has taken steps to protect individual privacy and mitigate the privacy

risks. Provide an example of how information is handled at each stage of the information life cycle. Also discuss privacy risks associated with the sharing of information outside of the agency and how those risks were mitigated. Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the agency.

Individual applicant and licensing information that is shared between the tribes, the NIGC and the FBI is transmitted over a network that is secured and encrypted using FIPS 140-2 validated encryption. Access to the information is limited to authorized NIGC and tribal personnel and this access is subject to credentialing and identity verification and personnel are mandated to receive annual Criminal Justice Information System (CJIS) security and awareness training. The NIGC maintains policies for the physical protection of information to protect the full lifecycle of the information from insider and outsider threats and maintains policies that outline the proper disposal, sanitization, and destruction of protected media.

All other collections are not routinely shared outside of the NIGC (see Section 2F) and are archived in dedicated document libraries (see Section 2D) that are secured and accessible to designated organizational units and security groups.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Describe how the use of the system or information collection relates to the purpose of the underlying mission of the organization. Is the information directly relevant and necessary to accomplish the specific purposes of the system? For Privacy Act systems, the Privacy Act at 5 U.S.C. 552a(e)(1) requires that each agency shall maintain in its records only such information about an individual that is relevant and necessary to accomplish an agency purpose required by statute or by executive order of the President.

☒ Yes: *Explanation*
☐ No

The NIGC's statutory mandate and agency regulations require that the NIGC:

- Oversee the process for employment and licensing of certain categories of tribal gaming personnel (CFR 556/558);
- Perform background investigations of persons involved in managing tribal gaming operations (CFR 537);
- Conduct investigations to monitor the compliance with the IGRA (CFR 571);

- Oversee the self-regulation of Class II gaming (CFR 518);
- Ensure that Indian gaming takes place on Indian lands (CFR 559);
- Hire staff as necessary (25 U.S.C. 2701).

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

Does the technology create new data or conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? Is data aggregated in a way that will permit system users to easily draw new conclusions or inferences about an individual? Electronic systems can sift through large amounts of information in response to user inquiry or programmed functions, or perform complex analytical tasks resulting in other types of data, matching, relational or pattern analysis, or reporting. Discuss the results generated by these uses and include an explanation on how the results are generated, whether by the information system or manually by authorized personnel. Explain the purpose and what will be done with the newly derived data. Derived data is obtained from a source for one purpose and then used to deduce/infer a separate and distinct bit of information to form additional information that is usually different from the original source information. Aggregation of data is the taking of various data elements and turning it into a composite of all the data to form another type of data, e.g., tables or data arrays.

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

Will the results or new data be placed in individuals' records? Explain in detail the purpose of creating the new data, how it will be used, by whom it will be used, with whom it will be shared, and any resulting effect on individuals.

☐ Yes: *Explanation*

☐ No

☒ N/A

D. Can the system make determinations about individuals that would not be possible without the new data?

Will the new data be used to make determinations about individuals or will it have any other effect on the subject individuals? Explain in detail the purpose of creating the new data, how it will be used, by whom it will be used, with whom it will be shared, and any resulting effect on individuals.

☐ Yes: *Explanation*

☐ No

☒ N/A

E. How will the new data be verified for relevance and accuracy?

Explain how accuracy of the new data is ensured. Describe the process used for checking accuracy. Also explain why the system does not check for accuracy. Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project.

N/A

F. Are the data or the processes being consolidated?

If the data is being consolidated, that is, combined or united into one system, application, or process, then the existing controls should remain to protect the data. If needed, strengthen the control(s) to ensure that the data is not inappropriately accessed or used by unauthorized individuals. Minimum sets of controls are outlined in OMB Circular A-130, Appendix III.

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

Describe the process by which an individual receives access to the information within the system. Explain what roles these individuals have and their level of access. If remote

access to the system is allowed or external storage or communication devices interact with the system, describe any measures in place to secure the transmission and storage of data (e.g., encryption and/or two-factor authentication). Do users have "read-only" access or are they authorized to make changes in the system? Also consider "other" users who may not be as obvious, such as the GAO or the Inspector General, database administrators, website administrators or system administrators. Also include those listed in the Privacy Act system of records notice under the "Routine Uses" section when a Privacy Act system of records notice is required.

☒ Users

NIGC Compliance personnel who oversee the gaming employment application process will have read access to information and reports. NIGC Contracts Background Investigators will have control over the information that they accumulate in the course of drafting their final reports. Final reports are shared with NIGC leadership. Information held in dedicated document libraries allow access to all members of the relevant security group.

☐ Contractors

☐ Developers

☒ System Administrator

IT Administrators have access to administrative controls that archive the information

☒ Other: *Describe*

Privacy and Records Information personnel (Agency Records Officer, FOIA Officer, Privacy Officer) have access as necessary to ensure records management oversight and compliance with the FOIA and Privacy Act.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Users are normally only given access to certain data on a "need-to-know" basis for information that is needed to perform an official function. Care should be given to avoid "open systems" where all information can be viewed by all users. System administrators may be afforded access to all of the data depending upon the system or application. However, access should be restricted when users may not need to have access to all the data. For more guidance on this, refer to the Federal Information Processing Standards [FIPS] Publications in the authorities.

Access to information for individuals is primarily determined by membership in an organizational unit and membership in a security group.

Organization units flow from the organization structure. At the primary organizational level, the NIGC is composed of the Office of the General Counsel and the Chief of Staff. Under the Chief of Staff there are 4 divisions (IT, Public Affairs, Finance, and Compliance) and under each division there are various sub-divisions. Upon onboarding, employees are granted access to specific information sub-systems and/or document libraries that are managed by division / sub-division record groups.

Security groups are created to enable the management of division / sub-division record groups but also can be created for other purposes.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

☐ No

Cloud products and services that will be provided as part of the installation of the system are FedRAMP certified. The NIGC uses contracted personnel on a limited basis and such contracts contain provisions for handling confidential information.

J. Is the system using technologies in ways that the NIGC has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

Are there new technologies used to monitor activities of the individual in any way? Access logs may already be used to track the actions of users of a system. Describe any new software being used, such as keystroke monitoring.

☒ Yes. *Explanation*

☐ No

The NIGC recently started employing multi-factor authentication for users for sign-on. New Microsoft 365 and Azure Active directory controls are employed with SPO document libraries to monitor activities of individuals on the file / folder level. The TIMS system has recently upgraded its user activity logs for enhanced monitoring.

K. Will this system provide the capability to identify, locate and monitor individuals?

Most systems now provide the capability to identify and monitor individual's actions in a system (e.g., audit trail systems/ applications). For example, audit logs may record username, time and date of logon, files accessed, or other user actions. Check system security procedures for information to respond to this question.

☒ Yes. *Explanation*

☐ No

The system generates audit logs that record IP address, username, time/date of logon, and files accessed.

Sub-systems also have various abilities to monitor activities and these activities are maintained in logs that are accessible to administrators.

L. What kinds of information are collected as a function of the monitoring of individuals?

Provide what audit activities are maintained to record system and user activity including invalid logon attempts and access to data. The IT Security A&A process requires a system security plan outlining the implementation of the technical controls associated with identification and authentication of users to the system. Examples of information collected may include username, logon date, number of failed logon attempts, files accessed, and other user actions on the system.

Monitoring includes logging and maintenance of system, application, and security events. The responsible designated IT Specialist reviews and analyzes system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings, and to take necessary actions.

Audit reviews and analysis of the following events are conducted once a week.

- Successful and unsuccessful system log-on attempts.
- Successful and unsuccessful attempts to use:
    - access permission on a user account, file, directory or other system resource;
    - create permission on a user account, file, directory or other system resource;
    - write permission on a user account, file, directory or other system resource;
    - delete permission on a user account, file, directory or other system resource;
    - change permission on a user account, file, directory or other system resource;

- Successful and unsuccessful attempts to change account passwords.
- Successful and unsuccessful actions by privileged accounts.
- Successful and unsuccessful attempts to:
    - access the audit log files;
    - modify the audit log files;
    - destroy the audit log file.

M. What controls will be used to prevent unauthorized monitoring?

Certain laws and regulations require monitoring for authorized reasons by authorized employees. Describe the controls in place to ensure that only authorized personnel can monitor use of the system. For example, business rules, internal instructions, posting Privacy Act Warning Notices address access controls, in addition to audit logs and least privileges. It is the responsibility of information system owners and system managers to ensure no unauthorized monitoring is occurring.

Monitoring systems and tools are controlled using role-based access to prevent unauthorized monitoring activities. The system owner approves and ensures least privilege access is implemented for users with access to these systems.

N. How will the PII be secured?

Discuss how each privacy risk identified was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included. Describe auditing features, access controls, and other possible technical and policy safeguards such as information sharing protocols, or special access restrictions. Do the audit features include the ability to identify specific records each user can access? How is the system audited? For example, does the system perform self-audits, or is the system subject to third party audits or reviews by the Office of Inspector General or Government Accountability Office (GAO). Does the IT system have automated tools to indicate when information is inappropriately accessed, retrieved or misused? Describe what privacy and security training is provided to system users. Examples of controls include rules of behavior, encryption, secured facilities, firewalls, etc.

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☒ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges

☐ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☐ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☐ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☒ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

Although all employees who have access to information in a Privacy Act system have responsibility for protecting and safeguarding that information, often the information system owner and Privacy Act system manager share the responsibility for protecting the privacy rights of employees and the public.

The Privacy Act Officer is responsible for processing Privacy Act requests. Procedures for making Privacy Act requests for are published at 25 C.F.R 515.3.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

This may be the information system owner and Privacy Act system manager, or may be another individual with designated responsibility, or otherwise stipulated by contract or in language contained in an agreement (e.g., Division Head or Program Manager). There may be multiple responsible officials. Consider a system that contains several databases from different program offices; there may be one information system owner and several Privacy Act system managers. Also, describe who is responsible for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information.

The NIGC Breach Response Plan outlines the roles, responsibilities and procedures in the event of a breach. NIGC authorized system users, employees, and contractors are required to immediately report a breach of PII to their supervisor, the NIGC Service Desk itsupport@nigc.gov, NIGC Information Security Officer (ISO) iso@nigc.gov and Senior Agency Officer for Privacy (SAOP) at privacy@nigc.gov. The SAOP is responsible for assessing privacy impacts and addressing notification and reporting issues.

Section 5. Review and Approval

PIAs must be signed by the designated Information System Owner, Agency Privacy Officer, and the Chief Information Officer as the Reviewing Official.

Information System Owner

Email: milton.cartwright@nigc.gov
First Name: Milton Last Name: Cartwright Jr. Title: Information Technology Manager
Bureau/Agency: NIGC Phone: (202) 632-7003 Date: October 26, 2023

Signature: Milton Cartwright Jr Digitally signed by Milton Cartwright Jr
Date: 2023.10.26 16:25:57 -04'00'

Privacy Officer

Email: tim.osumi@nigc.gov
First Name: Tim Last Name: Osumi Title: Agency Privacy Officer
Bureau/Agency: NIGC Phone: Date:

Signature: TIM OSUMI Digitally signed by TIM OSUMI
Date: 2023.10.31 16:58:57
-04'00'

Authorizing Official

Email:

First Name: Jun Last Name: Kim Title: Chief Information Officer
Bureau/Agency: NIGC Phone: Date:

Signature: JUN KIM Digitally signed by JUN KIM
Date: 2023.11.01 08:47:41
-04'00'