NIGC Compliance Plan for OMB Memorandum M-25-21, Accelerating Federal Use of AI through Innovation, Governance and Public Trust

September 2025

Version:1.1

Prepared by Tim Cotton, Chief Technology Officer and Chief Artificial Intelligence Officer

REVISION HISTORY

Date	Name	Description of Change	Version
09/22/2025	AI Governance Body	AI Compliance Plan per M-25-21	1.0
09/27/2025	AI Governance Body	AI Compliance Plan per M-25-21 updates	1.1

TABLE OF CONTENTS

Contents

PURPOSE

The Artificial Intelligence (AI) in Government Act of 2020[1] and OMB Memorandum M-25-21[2], *Accelerating Federal Use of AI through Innovation, Governance and Public Trust*, directs the National Indian Gaming Commission (NIGC) to submit to the Office of Management and Budget (OMB) and post publicly on its website either a plan to achieve consistency with M-25-21 or a written statement that the NIGC does not use and does not anticipate using covered AI.

This document outlines the National Indian Gaming Commission (NIGC)'s compliance plans that will satisfy the requirements of Section 3(b)(ii) of the Appendix to OMB Memorandum M-25-21 and Section 104(c) of the AI in Government Act. NIGC will report compliance with the individual use-case-specific practices mandated in Section 4 of M-25-21 Appendix separately through the annual AI use case inventory.

AUTHORITY

OMB mandates, Presidential Directives, and other federal regulations primarily guide the NIGC's AI policies. OMB mandates, such as the Federal Data Strategy, the Cloud Smart Strategy, and Accelerating Federal Use of AI through Innovation, Governance and Public Trust, provide a framework for leveraging data as a strategic asset and adopting modern technology practices, including AI. These authorities collectively empower federal agencies to develop and implement AI policies that align with national priorities, promote innovation, and maintaining the public trust in the use of AI technologies.

SCOPE

This AI Compliance plan applies to NIGC, including its employees and all third parties (such as consultants, vendors, and contractors) that use or access any information technology (IT) resources under the administrative responsibility of NIGC or its IT services. This encompasses systems managed or hosted by third parties on behalf of the NIGC.

This policy covers all technology systems that deploy AI technology, hereinafter called "AI systems". AI is a machine-based system that can make predictions, recommendations, or decisions influencing real or virtual environments for a given set of human-defined objectives. AI systems use machine and human-based inputs to perceive environments, abstract perceptions into models through automated analysis, and use model inference to formulate options for information or action. The definition includes systems using machine learning, large language models, natural language processing, computer vision technologies, and generative AI. It excludes basic calculations, basic automation, or pre-recorded "if this, then that" response systems.

[1] H.R.2575 - 116th Congress (2019-2020): AI in Government Act of 2020 | Congress.gov | Library of Congress
[2] M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf

This policy applies to all new and existing AI systems developed, used, or procured by NIGC, which could directly impact the mission or security of NIGC.

ABOUT NIGC

The National Indian Gaming Commission was created in 1988 with the passage of the Indian Gaming Regulatory Act (IGRA), which was enacted to support and promote tribal economic development, self-sufficiency, and strong tribal governments through the operation of gaming on Indian lands. The Act provides a statutory basis for the federal regulation of Indian gaming. IGRA establishes the Commission to regulate and support tribal gaming as a means of generating revenue for tribal communities. See 25 U.S.C. § 2704.

The Commission consists of three full-time members, including a Chair and two Associate Commissioners. The Chair is appointed by the President and confirmed by the Senate. The two Associate Commissioners are appointed by the Secretary of the Interior. The Commission selects a Vice Chair by a majority vote. At least two members of the Commission must be members of a federally recognized Indian Tribe and only two may be of the same political party.

The National Indian Gaming Commission is committed to fulfilling its responsibilities by:

- Regulating and monitoring certain aspects of Indian gaming;
- Coordinating its regulatory responsibilities with tribal regulatory agencies;
- Providing training and technical assistance to tribal regulatory agencies;
- Reviewing and approving tribal gaming ordinances and management agreements;
- Reviewing the backgrounds of individuals and entities to ensure the suitability of those seeking to manage or invest in Indian gaming;
- Overseeing and reviewing the conduct and regulation of Indian gaming operations;
- Enforcing violations against the IGRA and NIGCs regulations; and
- Referring criminal matters to appropriate tribal, Federal, and state law enforcement entities.

To achieve its Congressional mandate, the Commission adheres to the principles of good government, including transparency and NIGC accountability; promoting fiscal responsibility; operating with consistency and clarity to ensure fairness in the administration of the IGRA; and respecting the capabilities and responsibilities of each sovereign tribal nation in order to fully promote tribal economic development, self-sufficiency, and strong tribal governments.

DRIVING AI INNOVATION

NIGC is committed to fostering an environment where AI technologies can be used, developed, and deployed responsibly for the benefit of the NIGC. The foundation of NIGC's efforts to accelerate AI use is ensuring such advancements align with regulatory standards through the program described by this document. This AI strategy allows NIGC to leverage AI's full

potential while ensuring alignment with its mission, values, and regulatory requirements. NIGC's AI strategy will focus on integrating AI into its operations responsibly and effectively, driving innovation, and managing associated risks.

Removing Barriers to the Responsible Use of AI

One of NIGCs primary goals is to identify and mitigate barriers to the responsible use of AI. We have undertaken several initiatives to achieve this goal:

- **Barrier Identification:** Conduct reviews to identify barriers to AI adoption, including issues related to data access, technical infrastructure, and organizational readiness.
- **Mitigation Strategies:** Develop and implement strategies to address barriers, such as enhancing data governance frameworks, investing in AI infrastructure, and providing targeted staff training.
- **Resource Allocation:** Ensuring necessary resources, including staffing and budgetary resources, to support responsible AI use.

Currently, there are no explicit barriers to the responsible use of AI at NIGC. However, there are pressures that impact the adoption of any new capabilities that apply broadly and are not exclusive to AI:

- AI use cases compete for funding and staffing with other important priorities at the NIGC including investments in core NIGC capabilities, cyber security, and other use cases in its modernization agenda.
- Planning processes to allocate funding and staff resources typically requires a budget cycle to implement significant new initiatives.

NIGC simultaneously has some advantages in the adoption of AI and of non-safety, non-rights impacting AI:

- The NIGC deals predominantly with moderate sensitivity, open source, and commercially provided information.
- The NIGC technology is dominated by commercial off-the-shelf capabilities which are rapidly accreting useful AI as a natural extension of their capabilities.
- As a small NIGC, decision making is relatively nimble and speedy compared to larger organizations.

Currently NIGC is not experiencing any barriers with respect to its AI roadmap regarding access to necessary software tools, open-source libraries, and deployment and monitoring capabilities to rapidly develop, test, and maintain AI applications as the current focus on AI is oriented towards exploiting and taking advantage of AI features in commercial software and not the direct development of AI applications.

Sharing and Reuse

To ensure a consistent and unified approach to AI innovation, governance and trust, NIGC has taken steps to harmonize AI requirements across the NIGC:

- **Documentation of Best Practices:** Document and share best practices regarding AI governance, innovation, and risk management to ensure they are consistently applied.
- **Interagency Coordination:** Engaging in interagency coordination efforts to align NIGC AI strategies and policies with other federal agencies, promoting a coherent and collaborative approach to AI use.
- **Continuous Improvement:** NIGC AI practices and policies will be regularly updated to reflect emerging trends, technological advancements, and evolving regulatory requirements.

NIGC recognizes the importance of collaboration and knowledge sharing in advancing AI innovation. Currently, NIGC technology footprint is almost exclusively based on commercial software products with little to any modifications for NIGC. In the few places that NIGC is responsible for software development, the systems are primarily transaction processing in nature and do not currently rely on AI capabilities.

To the extent NIGC were to enter this space, its efforts would include:

- **Custom-Developed AI Code:** Ensuring that custom-developed AI code, including models and model weights, is shared consistent with M-25-21.
- **Coordination Efforts:** Coordinating with relevant offices within NIGC to facilitate sharing and collaboration, ensuring that best practices are disseminated and adopted across the organization.

AI Talent

Building and maintaining a skilled AI workforce is crucial for advancing responsible AI innovation. NIGC's initiatives in this area include:

- **Talent/Human Resource Planning:** As part of its annual human capital process, NIGC identifies strategic trends and emerging talent/human resources required to support NIGC's strategy. NIGC does not currently have an explicit strategy for recruiting individual AI talent. However, it will identify specific duties within position descriptions that are important for NIGC's acceleration of AI use.
- **Internal Training Programs:** NIGC's AI governance body is curating and promoting training programs to enhance AI skills within its existing workforce. These programs cover various topics, from basic AI literacy to advanced cyber amid generative AI topics
  NIGC has leveraged the capabilities of larger federal agencies, the Chief Artificial Intelligence Officer's Council (CAIOC), and user groups to coordinate for and plan employee training sessions based on their work roles (e.g., focusing on leadership, acquisition workforce, hiring teams, administrative personnel, or others).

IMPROVING AI GOVERNANCE

AI Governance Board

Establishing an AI governance body within NIGC is a critical component of the NIGC's

commitment to ensuring responsible use of AI technologies. This body is designed to oversee the implementation and operation of AI systems and ensure compliance with relevant laws, regulations, and internal policies.

The AI governance body at NIGC is comprised of representatives from key offices, ensuring a comprehensive and multidisciplinary approach to AI oversight. Leadership within NIGC on the governance body includes:

- Chief Information Officer
- Chief Information Security Officer
- Chief Technology Officer
- Chief of Public Affairs
- Chief of Staff
- General Counsel
- Chief Compliance Officer
- Chief Financial Officer
- Privacy & Records Information Management Officer

The AI governance body aims to achieve the following outcomes:

- **Risk Mitigation:** Identify and mitigate potential risks associated with AI, including poor operator or user practices, biases and other harms.
- **Transparency and Accountability:** Maintain transparency in AI operations and hold stakeholders accountable for their roles in AI governance.
- **Continuous Improvement:** Foster a culture of constant improvement in AI governance practices, keeping pace with technological advancements and emerging best practices.

The AI governance body will consult with external experts as appropriate and consistent with applicable laws to enhance the robustness of NIGC's AI governance framework. These consultations may include:

- **Interagency Collaboration:** Coordinating with other federal agencies to share knowledge and align best practices for AI governance.
- **Academic Institutions:** Collaborating with researchers and experts from universities and research institutions.
- **Industry Leaders:** Engaging with industry experts to gain insights into cutting-edge AI technologies and practices.

The AI governance body operates under a defined framework that includes regular meetings, a structured review process for AI projects, and transparent reporting lines to senior leadership. Key activities include:

- **Review and Approval:** Evaluating AI projects and use cases to ensure they meet legal and policy requirements before deployment.
- **Monitoring and Oversight:** Continuously monitoring AI systems for compliance and

performance, with mechanisms in place for regular reviews and audits.
- **Policy Development:** Developing and updating internal AI principles, guidelines, and policies to reflect the evolving AI landscape and regulatory requirements.
- **Stakeholder Engagement:** Ensuring active engagement with internal and external stakeholders to foster a collaborative approach to AI governance.

NIGC leverages the resources, controls, and governance capabilities of the Office of Chief Information Officer, the Chief Information Security Officer and Chief Technology Officer to ensure rigor operationalizing AI governance and compliance. This includes responsibility for the technology elements of the NIGC strategic plan, and various project governance and NIGC System Development Life Cycle (SDLC) policies where NIGC ensures various compliance requirements are brought to bear on NIGC technology.

NIGC Policies

After completing an inventory of AI use cases and assessing their implications, the NIGC will revise its NIGC policy to minimize operational and reputational consequences associated with the misuse of AI. Such policy will be reinforced by cybersecurity controls and through integration with project workflows so that safe AI deployment is approached as a business priority, and not just a technical consideration.

The NIGC cyber security program is routinely revised to incorporate the latest National Institute of Standards and Technology (NIST) controls including new control sets related to AI. The AI initiative to operationalize capabilities is further augmented by the NIGC's AI policy which fills policy and procedure gaps not addressed by modifications to existing policies.

As part of its fiscal 2026 policy and procedures review, updates will be made to existing policies to establish adequate safeguards and oversight mechanisms that allow generative AI to be used in the NIGC without posing undue risk. This includes updates to NIGC's Security Awareness Training program, and any SDLC policies and processes. In addition, the NIGC's IT Rules of Behavior and its Annual Security Awareness Training and Outreach plans will be updated to clarify expectations for staff interaction with open-source and licensed Generative AI capabilities which will be made readily accessible.

AI Use Case Inventory

NIGC will create and maintain an AI use case inventory to both understand how the NIGC uses AI and to manage AI deployments effectively, ensuring alignment with its mission and regulatory requirements.

NIGC is an independent regulatory agency with no sub-agencies or bureau components. NIGC is developing an AI policy and procedure and updating other key NIGC IT policies to:
- Ensure a clear understanding of what constitutes AI and a Use Case
- Develop a clear internal policy and process for periodically surveying the organization for AI use cases and routine review of use cases that aligns with requirements.
- Establish responsibility for submission and publication of use cases.

- Identify use cases that require special attention (e.g., rights and benefits impacting).
- Ensure previously excluded use cases are revisited periodically, as appropriate, for later inclusion.

NIGC's leverages established technology review processes and new and existing technology and IT investments within the Office of the Chief Information Officer. When there is an existing or planned introduction of AI, the office engages the AI governance body for appropriate follow-up.

To ensure NIGC's AI use case inventory is comprehensive and complete, NIGC further employs:

- **Education**: NIGC, through its AI governance body, will prepare basic education of the compliance requirements for AI that are now integrated into new staff onboarding and annual recurring Security Awareness Training. AI governance body members are further informed about more specific policies and procedures.
- **Stakeholder Engagement:** Engaging with key stakeholders, including Chief Information Security Officers, Chief Information Officers, Chief Technology Officers, and program managers to identify AI use cases.
- **Cross-functional Collaboration:** Collaborating across various departments ensures that all potential AI applications are captured and evaluated.
- **Documentation and Tracking:** Maintain detailed documentation and track all AI use cases to ensure they are accurately represented in the inventory.

While NIGC aims to maintain a transparent inventory of AI use cases, certain use cases may be excluded based on specific criteria:

- **Mission Risk:** Use cases that, if disclosed, could negatively impact, or create risks to the NIGC's mission, employees, customers, or the public.
- **Confidentiality Agreements:** Use cases subject to confidentiality agreements with other agencies, customers, employees, or stakeholders.
- **Security Concerns:** Use cases that involve sensitive or classified information that cannot be publicly disclosed.

NIGC is committed to periodically revisiting and validating AI use cases in its inventory to ensure accuracy and relevance. This process includes:

- **Periodic Reviews:** Conducting no less than annual reviews of the AI use case inventory to identify any changes or updates needed.
- **Validation Criteria:** Predefined criteria are used to reassess use cases and determine whether previously excluded cases should be included or whether any new cases meet the exclusion criteria.
- **Approval and Oversight:** The Chief Technology and AI Officer (CAIO) and the AI governance body is engaged in the review and validation process to ensure accountability and transparency.

In line with its commitment to transparency, NIGC will make AI use case inventories, according to the reporting guidance, publicly available on its website. The inventory will be updated no less than annually to reflect new AI use cases and any changes to existing ones. NIGC's public inventory includes:

- **Descriptions of AI Use Cases:** Provide clear and concise explanations of each AI use case, including its purpose, scope, and expected outcomes.
- **Compliance Information:** Provide designated compliance information per M-25-21 and any other subsequent standards.

The main clearinghouse for documenting and sharing best practices is the AI governance body and its members who participate, not only in sharing CAIOC community information, but also are participating in communities of interest for their discipline.

The NIGC CIO, CISO and CTO are members of the Small Agency CIO and CISO council, Federal Privacy Council, and members of DHS/CISA communities.

Other key NIGC officials, the Chief Compliance Officer, Office of General Counsel, Chief Financial Officer, are members of federal user groups and private sector organizations that, like the technology community, share developing AI best practices, risks and innovation through the lens of their function and professional area of responsibility.

FOSTERING PUBLIC TRUST IN FEDERAL USE OF AI

Determinations of Presumed High-Impact AI

To ensure the responsible deployment of AI, NIGC has established a process for determining which AI use cases are considered safety-impacting or rights-impacting:

- **Review Process:** Each current and planned AI use case undergoes a review to assess whether it matches the definitions of safety-impacting or rights-impacting AI defined in Section 5 of OMB Memorandum M-25-21.
- **Criteria for Assessment:** NIGC's assessment criteria include the potential for physical harm, the impact rights or benefits, and the degree of automation in decision-making processes.
- **Supplementary Criteria:** NIGC may develop additional criteria tailored to its specific operations to guide safety and rights-impacting AI decisions.

As described above, the NIGC AI governance body is tasked with ensuring the proper development and implementation of use case identification and review which also includes rights and safety impacting scenarios. The AI policy and related procedures ensure a comprehensive review by NIGC stakeholders.

Implementation of Risk Management Practices and Termination of Non-Compliant AI

Implementing effective risk management practices is essential to mitigate the risks associated

with AI. NIGC's AI policy will ensure:

- **Comprehensive Risk Assessments:** Conduct comprehensive risk assessments for all AI applications, identifying potential hazards, vulnerabilities, and impact on stakeholders.
- **Minimum Risk Management Practices:** Document and validate the implementation of minimum risk management practices, including data privacy, security measures, and contractual considerations.
- **Risk Management Framework:** Develop and maintain a risk management framework that outlines the procedures for identifying, assessing, mitigating, and monitoring risks throughout the AI lifecycle.

The NIGC has updated its process to NIGC staff regarding the contents of M-25-21 and the importance of clauses in M-25-21 regarding its obligations to protect the NIGC from non-compliant safety-impacting or rights-impacting AI from being deployed to the public.

NIGC's AI governance body who has a working understanding of M-25-21 as well as close working relationship with the CIO and CISO on compliance with various technical mandates regarding the procurement of technology for the NIGC.

Outreach and training to the general staff of the NIGC sponsored by the AI governance body includes key compliance elements related to M-25-21 as well as other federal mandates regarding the use of AI.

In certain circumstances, it may be necessary to issue waivers for one or more of the minimum risk management practices. NIGC, as part of its AI policy, has outlined a straightforward process for this:

- **Criteria for Waivers:** Develop criteria to guide the decision to waive risk management practices, ensuring that waivers are granted only when necessary and justified.
- **Issuance and Revocation:** Establish procedures for issuing, denying, revoking, tracking, and certifying waivers, with oversight from the Chief AI Officer (CAIO) and the AI governance body.
- **Documentation and Transparency:** Maintain detailed records of all waiver decisions to ensure transparency and accountability.

As of the date of this plan, NIGC has no AI use cases requiring a waiver. As part of the NIGC's normal policy review process, NIGC's AI policy and associated risk management practices will be updated as we develop maturity in this space.

APPENDIX A: TERMS AND DEFINITIONS

Artificial Intelligence (AI) is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems use machine and human-based inputs to perceive real and virtual environments, abstract such perceptions into models through analysis, and use model inference to formulate options for information or action.

Chief Technology/AI Officer (CAIO): A senior executive responsible for overseeing the NIGC's development and implementation of AI strategies, policies, and governance. The CAIO ensures compliance with standards and regulatory requirements and coordinates AI initiatives across the organization.

Chief AI Officer Council (CAIOC): An interagency group led by OMB and comprised of NIGC CAIOs to support the roll-out of M-25-21 and share best practices for the implementation of AI strategies, policies, and governance. The CAIOC also assists in coordinating AI initiatives across the Federal Government.

AI Governance is the framework, processes, and policies implemented to ensure the ethical, legal, and responsible use of AI within an organization. It includes establishing governance bodies, principles, and guidelines to oversee AI applications.

AI Governance Body: A multidisciplinary committee comprising representatives from key offices within the NIGC. This committee is responsible for overseeing the implementation and operation of AI systems. The governance body ensures that AI initiatives align with standards, regulatory requirements, and the NIGC's strategic goals.

AI Use Case Inventory: A comprehensive list of all AI applications and use cases within an organization, detailing their purpose, scope, and compliance with regulatory standards. The inventory is used to manage AI deployments effectively and ensure transparency.

Rights-Impacting AI: AI applications that can potentially affect individuals' civil rights, privacy, or other fundamental rights. These use cases require careful consideration of their implications and compliance with legal and regulatory requirements.

Generative AI: A class of AI models that emulate the structure and characteristics of input data to generate derived synthetic content, such as images, videos, audio, text, and other digital content.

Risk Management Framework: A structured approach for identifying, assessing, mitigating, and monitoring risks associated with AI applications. The framework includes preventive controls, monitoring mechanisms, and procedures for managing incidents and non-compliance.

Transparency and Accountability: Principles ensuring that the development and deployment of AI systems are open and transparent, with clear documentation and oversight to hold stakeholders accountable for their roles in AI governance.

Responsible AI Use: The capabilities to innovate and promote the responsible adoption, use, and continued development of AI, while ensuring appropriate safeguards are in place to protect privacy, civil rights, and civil liberties, and to mitigate any unlawful discrimination, consistent with the AI in Government Act.

AI Talent Development: Initiatives and programs that aim to build and maintain a skilled AI workforce through targeted recruitment, training, and career development opportunities.

Technology Review Process: A formal procedure for evaluating technology requests, including AI applications, to ensure they meet technical, ethical, and regulatory standards before approval and implementation.