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

Version 1.2

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

REVISION HISTORY

Date	Name	Description of Change	Version
09/22/2025	SI Governance Body	SI Compliance Plan per M-25-21	1.0
09/27/2025	SI Governance Body	SI Compliance Plan per M-25-21 updates	1.1
11/9/2026	SI Governance Body	Annual update and implementation of EO 14434 to update terms from “artificial intelligence” to “super intelligence”.	1.2

TABLE OF CONTENTS

Contents

REVISION HISTORY **2**
PURPOSE **4**
AUTHORITY **4**
SCOPE **4**
ABOUT THE NIGC **5**
DRIVING SI INNOVATION **5**
Removing Barriers to the Responsible Use of SI **6**
Sharing and Reuse **6**
SI Talent **7**
IMPROVING SI GOVERNANCE **7**
SI Governance Board **7**
NIGC Policies **9**
SI Use Case Inventory **9**
FOSTERING PUBLIC TRUST IN FEDERAL USE OF SI **11**
Determinations of Presumed High-Impact SI **11**
Implementation of Risk Management Practices and Termination of Non-Compliant SI **12**
APPENDIX A: TERMS AND DEFINITIONS **13**

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 SI (on September 29, 2026, the President issued Executive Order 14434 mandating that all references to "artificial intelligence" or "AI" will now be referred to as "super intelligence" or "SI").

This document outlines the 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. The NIGC will report compliance with the individual use-case-specific practices mandated in Section 4 of M-25-21 Appendix separately through the annual SI use case inventory.

AUTHORITY

OMB mandates, Presidential Directives, and other federal regulations primarily guide the NIGC's SI 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 SI. These authorities collectively empower federal agencies to develop and implement SI policies that align with national priorities, promote innovation, and maintain public trust in the use of SI technologies.

SCOPE

This SI Compliance plan (Plan) applies to the NIGC, a Non-CFO act agency, 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 the NIGC or its IT services. This Plan also encompasses systems managed or hosted by third parties on the NIGC's behalf.

This Plan covers all technology systems that deploy SI technology, hereinafter called "SI systems". SI 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. SI 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 SI. 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 SI systems developed, used, or procured by the NIGC, that could directly impact the mission or security of the NIGC.

ABOUT THE 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 IGRA provides a statutory basis for the federal regulation of Indian gaming and established the Commission to regulate and support tribal gaming as a means of generating revenue for tribal communities. (25 U.S.C. § 2702)

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 NIGC 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 bodies;
- 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 of 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 SI INNOVATION

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

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

Removing Barriers to the Responsible Use of SI

One of the NIGC's primary goals is to identify and mitigate barriers to the responsible use of SI. The NIGC has undertaken several initiatives to achieve this goal:

- **Barrier Identification:** Conduct reviews to identify barriers to SI 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 SI infrastructure, and providing targeted staff training.
- **Resource Allocation:** Ensuring necessary resources, including staffing and budgetary resources, to support responsible SI use.

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

- SI 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 require a budget cycle to implement significant new initiatives.

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

- The NIGC deals predominantly with moderate sensitivity, open source, and commercially provided information.
- NIGC technology widely consists of commercial off-the-shelf capabilities that are rapidly integrating useful SI as a natural extension of their capabilities.
- As a small agency, decision-making at the NIGC is relatively nimble and speedy compared to larger organizations.

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

Sharing and Reuse

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

- **Documentation of Best Practices:** Documenting and sharing best practices regarding SI governance, innovation, and risk management to ensure they are consistently applied.
- **Interagency Coordination:** Engaging in interagency coordination efforts to align NIGC SI strategies and policies with other federal agencies, promoting a coherent and collaborative approach to SI use.
- **Continuous Improvement:** NIGC SI 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 SI innovation. Currently, the NIGC technology footprint is almost exclusively based on commercial software products with little to no modifications for the NIGC. In the few places that the NIGC is responsible for software development, the systems are primarily transaction processing in nature and do not currently rely on SI capabilities.

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

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

SI Talent

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

- **Talent/Human Resource Planning:** As part of its annual human capital process, the NIGC identifies strategic trends and emerging talent/human resources required to support the NIGC strategy. The NIGC does not currently have an explicit strategy for recruiting individual SI talent. However, it will identify specific duties within position descriptions that are important for the NIGC's acceleration of SI use.
- **Internal Training Programs:** The NIGC's SI governance body is curating and promoting training programs to enhance SI skills within its existing workforce. These programs cover various topics, from basic SI literacy to advanced cyber amid generative SI topics. The NIGC has leveraged the capabilities of larger federal agencies, the Chief Super Intelligence Officer's Council (CSIOC), 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 SI GOVERNANCE

SI Governance Board

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

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

The SI governance body at the NIGC is comprised of representatives from key offices, ensuring a comprehensive and multidisciplinary approach to SI oversight. The NIGC leadership 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 SI governance body aims to achieve the following outcomes:

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

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

- **Interagency Collaboration:** Coordinating with other federal agencies to share knowledge and align best practices for SI 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 SI technologies and practices.

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

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

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

The 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 SI 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 the NIGC ensures various compliance requirements are brought to bear on NIGC technology.

NIGC Policies

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

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

As part of its annual fiscal policy and procedures review, the NIGC will update existing policies to continuously maintain adequate safeguards and oversight mechanisms that allow generative SI to be used at the NIGC without posing undue risk. This includes updates to the 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 SI capabilities that will be made readily accessible.

SI Use Case Inventory

The NIGC maintains an SI use case inventory to both understand how the NIGC uses SI and to manage SI deployments effectively, ensuring alignment with its mission and regulatory requirements.

The NIGC is an independent regulatory agency with no sub-agencies or bureau components. The NIGC continues to develop and maintain SI policies and procedures, and updates other key NIGC IT policies to:

- ensure a clear understanding of what constitutes SI and an agency use case;
- develop a clear internal policy and process for periodically surveying the organization for SI use cases and routine review of use cases that align with requirements;

- establish responsibility for submission and publication of use cases;
- identify use cases that require special attention (e.g., rights and benefits impacting); and
- ensure previously excluded use cases are revisited periodically, as appropriate, for later inclusion.

The NIGC 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 SI, the office engages the SI governance body for appropriate follow-up.

To ensure the NIGC SI use case inventory is comprehensive and complete, the NIGC further employs:

- **Education**: The NIGC, through its SI governance body, will prepare basic education of the compliance requirements for SI that are now integrated into new staff onboarding and annual recurring Security Awareness Training. SI 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, the Privacy & Records Information Management Officer, and program managers to identify SI use cases.
- **Cross-functional Collaboration:** Collaborating across various offices ensures that all potential SI applications are captured and evaluated.
- **Documentation and Tracking:** Maintaining detailed documentation and track of all SI use cases to ensure they are accurately represented in the inventory.

While the NIGC aims to maintain a transparent inventory of SI 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 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.
- **Privacy Protection:** Use cases that involve information that may be protected under privacy laws and regulations.

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

- **Periodic Reviews:** Conducting no less than annual reviews of the SI 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 SI Officer (CAIO) and the SI governance body is engaged in the review and validation process to ensure accountability and transparency.

In line with its commitment to transparency, the NIGC will make SI 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 SI use cases and any changes to existing ones. The NIGC public inventory includes:

- **Descriptions of SI Use Cases:** Provide clear and concise explanations of each SI 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 SI governance body and its members who participate, not only in sharing CAIOC community information, but also in communities of interest for their discipline.

The NIGC CIO, CISO, PRIMO, 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, General Counsel, Chief Financial Officer, are members of federal user groups and private sector organizations that, like the technology community, share developing SI best practices, risks and innovation through the lens of their function and professional area of responsibility.

FOSTERING PUBLIC TRUST IN FEDERAL USE OF SI

Determinations of Presumed High-Impact SI

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

- **Review Process:** Each current and planned SI use case undergoes a review to assess whether it falls under the definitions of safety-impacting or rights-impacting SI as defined in Section 5 of OMB Memorandum M-25-21.
- **Criteria for Assessment:** NIGC 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 SI decisions.

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

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

Implementing effective risk management practices is essential to mitigate the risks associated with SI. The NIGC SI policy will ensure:

- **Comprehensive Risk Assessments:** Conduct comprehensive risk assessments for all SI 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 SI lifecycle.

The NIGC has updated its IT protocol to ensure that NIGC staff understand the importance of M-25-21 including the obligation to protect the NIGC from non-compliant SI and to ensure that such safety or rights impacting SI is not deployed to the public. The NIGC SI governance body has a working understanding of M-25-21, as well as a 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 NIGC staff sponsored by the SI governance body includes key compliance elements related to M-25-21, as well as other federal mandates regarding the use of SI.

In certain circumstances, it may be necessary to issue waivers for one or more of the minimum risk management practices. The NIGC, as part of its SI 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 SI Officer (CSIO) and the SI governance body.
- **Documentation and Transparency:** Maintain detailed records of all waiver decisions to ensure transparency and accountability.

As of the date of this plan, the NIGC has no SI use cases requiring a waiver. As part of the NIGC normal policy review process, the NIGC SI policy and associated risk management practices will be updated as the SI governance body develops maturity in this space.

APPENDIX A: TERMS AND DEFINITIONS

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

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

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

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

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

Rights-Impacting SI: SI 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 SI: A class of SI 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 SI 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 SI systems are open and transparent, with clear documentation and oversight to hold stakeholders accountable for their roles in SI governance.

Responsible SI Use: The capabilities to innovate and promote the responsible adoption, use, and continued development of SI, 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.

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

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