NARA 2025 AI Compliance Plan for OMB Memorandum M-25-21

September 18, 2025

- **Prepared by:** Gulam Shakir, Chief Artificial Intelligence Officer (CAIO)
- **Issued by:** Jim Byron, Senior Advisor to the Archivist of the United States

1. Introduction and Background

This document outlines the National Archives and Records Administration's (NARA) plan to achieve consistency with Office of Management and Budget (OMB) Memorandum M-25-21, "Accelerating Federal Use of AI through Innovation, Governance, and Public Trust." NARA is committed to leveraging Artificial Intelligence (AI) to advance its core mission of preserving and providing access to the nation's historical records. This plan details our strategy for driving responsible AI innovation, strengthening AI governance, and fostering public trust in our use of this transformative technology.

2. Driving AI Innovation

NARA will invest in AI research and development to advance responsible AI technologies. We will leverage the existing Enterprise Architecture Governance Board (EAGB) to review and assess the ethical implications of AI projects, develop clear AI Ethics Guidelines, collaborate with external stakeholders to share best practices, and conduct periodic audits and assessments of AI systems to ensure compliance.

2.1. Removing Barriers to the Responsible Use of AI

NARA has instituted a comprehensive strategy to address potential barriers to the responsible use of Artificial Intelligence, ensuring that all AI implementations align with our core mission, federal mandates, and ethical principles.

- **Barrier: Data Quality and Sensitivity.** Our vast and varied holdings present unique challenges, including inconsistent data formats, OCR errors from legacy scans, and the presence of PII.
    - **Mitigation:** We are actively improving data quality through targeted initiatives, applying advanced OCR models, and integrating automated PII detection tools into our data pipelines to ensure privacy by design.
- **Barrier: Model Transparency and Bias.** The "black box" nature of some AI models can be at odds with our need for transparent, auditable, and unbiased decision-making.
    - **Mitigation:** We mandate the use of Explainable AI (XAI) techniques where feasible and subject all AI systems used for augmenting records review to a human-in-the-loop validation process.
- **Barrier: Workforce Skills Gaps.** The specialized skills required for AI development, oversight, and management are in high demand.
    - **Mitigation:** NARA will mitigate this barrier through a multi-pronged workforce development strategy that includes upskilling internal talent and fostering a culture of continuous learning.

Providing Access to AI Development and Deployment Capabilities: To ensure our teams can rapidly and securely develop, test, and maintain AI applications, NARA has established a FedRAMP-authorized hybrid-cloud environment, provides access to a curated repository of approved open-source libraries, and will implement a secure MLOps pipeline for automated deployment and monitoring.

2.2. Sharing and Reuse of AI Assets

NARA's Chief Artificial Intelligence Officer (CAIO), in close partnership with the Chief Technology Officer (CTO), Chief Data Officer (CDO), and Chief Information Security Officer (CISO), spearheads NARA's internal coordination for all AI-related assets. Our strategy is centered on three components:

- **Centralized Inventories:** The CAIO maintains NARA's AI Use Case Inventory to provide all offices with visibility into ongoing and planned AI projects.
- **Shared Technical Platforms:** Information Services manages a centralized code repository (Git) for version-controlled AI/ML source code.
- **Governance and Standards:** The EAGB will set standards for documentation and quality to ensure shared assets are reliable and ready for reuse.

To further accelerate this activity, NARA has identified a need for dedicated AI Platform or MLOps Engineers and a dedicated funding stream for maintaining shared AI platforms.

2.3. Enhancing AI Talent

NARA is exploring opportunities to upskill existing staff and foster internal AI communities to create a new generation of archivists and data scientists.

- **Critical AI Skillsets Needed:** NARA requires a blend of core AI competencies, including Natural Language Processing (NLP), Computer Vision (CV), Machine Learning Engineering & MLOps, Data Science & Predictive Analytics, and AI Ethics & Governance.
- **Planned and In-Progress Initiatives:** We are implementing a comprehensive strategy to enhance AI talent through a combination of upskilling, training, collaboration, and experiential learning. This includes strategic partnerships, specialized skill development in areas like prompt engineering, leveraging federal resources from GSA and OMB, fostering an internal AI Community of Practice, and participating in cross-agency bodies like the CDO and AI Councils.

3. Improving AI Governance

3.1. AI Governance Board

In alignment with OMB M-25-21, NARA will initially leverage its Enterprise Architecture Governance Board (EAGB) to fulfill the functions of the AI Governance Board. This practical approach utilizes the EAGB's existing membership of business, technical, policy, and compliance representatives from offices including Agency Services, OCIO, General Counsel, Research Services, and Presidential Libraries. The EAGB will formalize governance, develop AI policies, conduct risk assessments, ensure transparency, foster collaboration, and consult with external experts. NARA may establish a dedicated AI Governance Board in the future as the agency's AI program matures.

3.2. Agency Policy Updates

In accordance with OMB Memorandum M-25-21, NARA is reviewing its IT policies to ensure our internal principles and guidelines are fully consistent with the federal framework. This review spans IT infrastructure, data governance, and cybersecurity to address the unique risks introduced by AI systems. The outcome will be a set of updated internal policies that enable secure, ethical, and effective AI innovation.

3.3. Guidance on the Use of Generative AI

NARA has developed internal guidance for employees and contractors on the use of an approved generative AI assistant. The guidance establishes robust safeguards and oversight mechanisms, including:

- **Safeguards:** Prohibiting the use of classified or sensitive data (PII, CUI), forbidding "High-Impact AI" use cases without CAIO approval, ensuring the tool is configured within our security boundary, and limiting its use to agency business only.
- **Oversight Mechanisms:** Requiring human review and validation for all AI-generated outputs, conducting continuous evaluation of the tool's performance and accuracy, providing a formal incident reporting process, and ensuring the policy is reviewed and updated periodically.

3.4. AI Use Case Inventory

The Office of the CAIO leads the maintenance of NARA's AI Use Case Inventory. We are formalizing this process by implementing a centralized intake form and creating a Standard Operating Procedure (SOP) for the inventory's lifecycle management. This SOP will define the process for updating use cases, such as when a model is approved for production or its risk designation changes.

4. Fostering Public Trust in Federal Use of AI

4.1. Determinations of High-Impact AI

NARA will establish a cross-functional team, led by the CAIO, to review each AI use case and determine if it is high-impact, in direct alignment with OMB M-25-21. NARA currently has no AI use cases that meet the definition of high-impact, and given our mission, we do not anticipate many will fall into the presumed high-impact categories. However, we are committed to vigilantly monitoring all future proposals and will rigorously apply all required safeguards for any use case that meets the criteria.

4.2. AI Risk Management Waiver Process

NARA is committed to upholding all minimum risk management practices. While M-25-21 allows for waivers in exceptional circumstances, they will be approached with the utmost scrutiny. Our CAIO holds the sole, non-delegable authority to review and issue a waiver, and will only do so with a clear, written determination that adhering to a practice would increase risk or impede critical operations. All waivers will be centrally tracked, certified annually, reported to OMB within 30 days, and publicly disclosed.

4.3. Implementation and Oversight of AI Risk Management

NARA will document AI risk management efforts through clear procedures, detailed risk registers, and comprehensive audit reports. The validation of these practices will be achieved through technical reviews, cybersecurity reviews (including SAST and DAST scanning), and continuous monitoring of AI systems.

4.4. Deployment Controls for High-Impact AI

NARA will establish a rigorous, multi-layered control system to prevent non-compliant high-impact AI from being deployed. This process requires a comprehensive risk assessment by the system owner, a mandatory independent validation by technical and cybersecurity teams, and formal, written risk acceptance from a designated senior official before any high-impact system can be deployed.

4.5. Termination Process for Non-Compliant AI

NARA will follow a strict "hard stop" policy. If a system is found to be non-compliant with mandated risk management practices at any point, its deployment or use will be immediately halted. The system will not be able to proceed until the non-compliance is fully remediated and has been re-validated through the same rigorous review process.

5. Conclusion

This AI Compliance Plan outlines NARA’s commitment to the responsible and innovative use of Artificial Intelligence. By strengthening our governance, investing in our workforce, and implementing robust risk management practices, we will ensure that our use of AI is transparent, ethical, and effective in advancing our mission to serve the American public. We will continue to refine this plan as the field of AI evolves and as we gain more experience with its practical applications within NARA.