Artificial Intelligence at USDA and PPQ

Guidance and directions for use and risk management

Kellyn Babbitt, PhD
APHIS-PPQ
kellyn.babbitt@usda.gov

Outline

AI in the US Government

White House OMB Memos

GSA Procurement of AI Technology

AI Use Case Inventory

USDA AI Strategy FY25-26

USDA Interim Guidance on Generative AI

Generative AI Acceptable Use Guidelines

What's happening with AI in PPQ

AI in the US Government

AI in Government Act of 2020

Created General Services Administration (GSA) AI Center of Excellence

Required White House Office of Management and Budget (OMB) guidance memos

Workforce development

Advancing American AI Act 2021

Required federal agency AI strategies

America's AI Action Plan 2025

Emphasizes rapid federal AI adoption and securing infrastructure for AI – data centers, energy

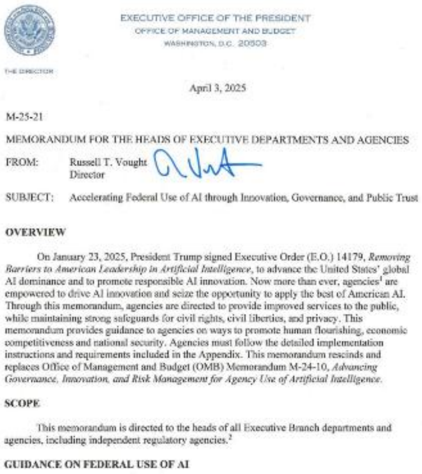
Multiple Executive Orders

Focused on removing barriers, promoting innovation, and adoption

White House OMB Memos in 2025

Memos include directives for all agencies to develop policies and strategies for agency AI use and procurement

M-25-21 - *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

April 3, 2025

M-25-21

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Russell T. Vought
Director

SUBJECT: Accelerating Federal Use of AI through Innovation, Governance, and Public Trust

OVERVIEW

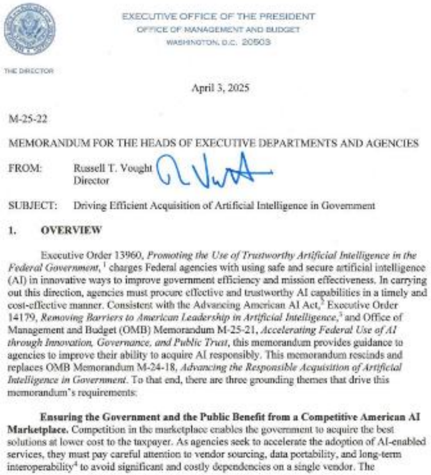
On January 23, 2025, President Trump signed Executive Order (E.O.) 14179, *Removing Barriers to American Leadership in Artificial Intelligence*, to advance the United States' global AI dominance and to promote responsible AI innovation. Now more than ever, agencies[1] are empowered to drive AI innovation and seize the opportunity to apply the best of American AI. Through this memorandum, agencies are directed to provide improved services to the public, while maintaining strong safeguards for civil rights, civil liberties, and privacy. This memorandum provides guidance to agencies on ways to promote human flourishing, economic competitiveness and national security. Agencies must follow the detailed implementation instructions and requirements included in the Appendix. This memorandum rescinds and replaces Office of Management and Budget (OMB) Memorandum M-24-10, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence*.

SCOPE

This memorandum is directed to the heads of all Executive Branch departments and agencies, including independent regulatory agencies.[2]

GUIDANCE ON FEDERAL USE OF AI

M-25-22 - *Driving Efficient Acquisition of Artificial Intelligence in Government*



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

April 3, 2025

M-25-22

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Russell T. Vought
Director

SUBJECT: Driving Efficient Acquisition of Artificial Intelligence in Government

1. OVERVIEW

Executive Order 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*,[1] charges Federal agencies with using safe and secure artificial intelligence (AI) in innovative ways to improve government efficiency and mission effectiveness. In carrying out this direction, agencies must procure effective and trustworthy AI capabilities in a timely and cost-effective manner. Consistent with the Advancing American AI Act,[2] Executive Order 14179, *Removing Barriers to American Leadership in Artificial Intelligence*,[3] and Office of Management and Budget (OMB) Memorandum M-25-21, *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*, this memorandum provides guidance to agencies to improve their ability to acquire AI responsibly. This memorandum rescinds and replaces OMB Memorandum M-24-18, *Advancing the Responsible Acquisition of Artificial Intelligence in Government*. To that end, there are three grounding themes that drive this memorandum's requirements:

Ensuring the Government and the Public Benefit from a Competitive American AI Marketplace. Competition in the marketplace enables the government to acquire the best solutions at lower cost to the taxpayer. As agencies seek to accelerate the adoption of AI-enabled services, they must pay careful attention to vendor sourcing, data portability, and long-term interoperability[4] to avoid significant and costly dependencies on a single vendor. The

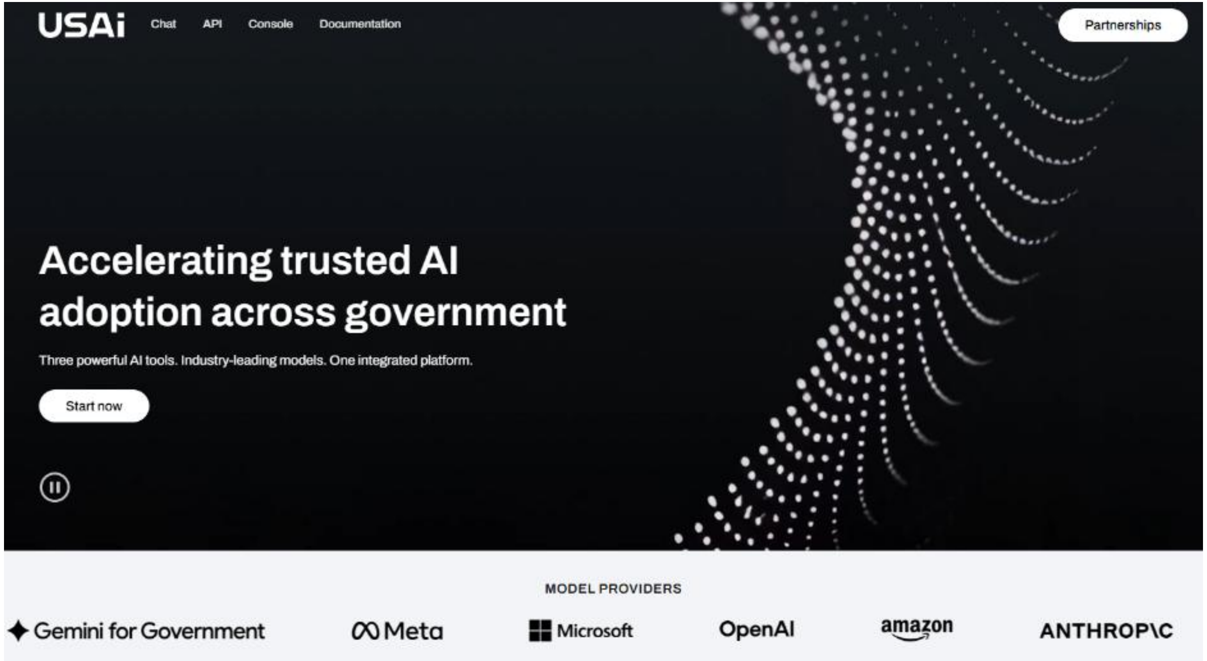
GSA procurement of AI technology

USAi API and Chatbot

Provides secure access to multiple major large language models (LLMs)

Agencies must sign MOU with GSA, 6-month free trial

Being evaluated by USDA, not currently approved for use



Accelerating trusted AI adoption across government

Three powerful AI tools. Industry-leading models. One integrated platform.

United States Department of Agriculture
Animal and Plant Health Inspection Service

AI Use Case Inventory

Annual Reporting

All agencies must report AI use to the White House OMB and the public

Productivity use cases are reported collectively

- Such as summarizations, time tracking, scheduling, email management, code generation, creating visualizations, etc.

Types of Use Cases

Includes in-house or third-party use cases at any development stage

Excludes security or intelligence use cases

Excludes basic or applied research unless intended for agency operations

High Impact Use Cases

Identifies use cases impacting civil rights or safety

Additional requirements for impact assessment and risk management

USDA AI Strategy FY25-26

Updated USDA AI Strategy expected Oct 2025

Current Goals:

- **AI Governance and Leadership:** Establish robust governance that fosters innovation, collaboration, and responsible use of AI.
- **Workforce Readiness:** Develop and recruit workforce with AI skills that anticipate and meet program needs.
- **Infrastructure and Tools:** Develop secure, scalable infrastructure for trustworthy, high-impact, innovative AI use.
- **Data Readiness and Access:** Provide guidance on data stewardship, support effective data use, and build confidence in AI outputs.
- **Ethical, Equitable, and Responsible AI Use:** Adopt policies to protect rights and safety and mitigate risks.

USDA Policy on Generative AI vs. Traditional AI

- Risks of Generative AI
  - Generation of inaccurate or outdated information
  - Hallucinations
  - Lack of data privacy
  - Potential misuse
- Restrictions on Generative AI
  - Prohibited within USDA unless reviewed and approved
- Traditional AI Usage
  - No restrictions except when rights- or safety-impacting

	Traditional	**Generative**
Approach	Deterministic, rule-based, structured tasks	Probabilistic and deep learning to generate new outputs
Applications	Automation, robotics, diagnostics, fraud detection	Chatbots, code development, drafting documents, website development, media creation
Learning mechanism	Direct programming of algorithms	Reinforcement learning and deep neural networks for autonomous learning from data
Advantages	Predictable, reliable, consistent outputs, explainable	Enhances creativity, addresses messy problems
Limitations	Limited to uses with clear rules, not flexible for handling undefined scenarios	Ethical concerns around creating realistic fake and/or false content, not explainable, outputs vary

USDA Interim Guidance on Generative AI

Updated Departmental Regulation on Generative AI expected Dec 2025

Generally Prohibits Generative AI Use

- Generative AI use requires prior written approval for use on USDA network
- Publicly available, third-party tools will be blocked

Generative AI Review Board (GAIRB)

- Established to review and grant exceptions for Generative AI use cases
- Approval based on needs of USDA

Extra Scrutiny for Specific Use Cases

- Involving PII, safety, rights, privileged access, or data transfer to systems without USDA authority to operate

Restricts Use for Providing USDA Services and Programs

- Not allowed for language translation or interpretation for providing services to USDA applicants and participants
- Considered high risk of providing erroneous information

Prohibits Submitting Protected Information

- Submission of PII or non-public information to a public Generative AI tool constitutes prohibited release of protected information

Unacceptable Uses

- Shall not be used to generate malicious, inappropriate, or illegal material

USDA Generative AI Acceptable Use Guidelines: **General Principles**

Accountability

Users are responsible for quality, accuracy, and reliability of work products and must be manually reviewed for errors and biases

Transparency

Users must disclose use of Generative AI and label outputs

Explainability

Users must ensure Generative AI outcomes are explainable by subject matter experts and others

Public Trust

Users are responsible for avoiding inappropriate, offensive, or illegal material and ensuring outputs align with USDA values and standards

Human Oversight

Users must maintain human validation and intervention protocols to ensure decisions influenced by Generative AI are evaluated

USDA Generative AI Acceptable Use Guidelines: **Data Protection and Privacy**

Prohibited Data for Public Tools

Users may not input non-public, restricted information into public Generative AI tools

Permitted Data for Internal Tools

When using USDA Generative AI tools, user may only input data up to the allowable sensitivity level of the specific tool

Data and Records Retention

Outputs of Generative AI may be considered federal records and must be treated as such

USDA Generative AI Acceptable Use Guidelines: **Unacceptable Uses**

Inherently Governmental Functions

Such as final hiring decisions, grant scoring and reviewing, or enforcement actions

Misinformation

Creation of false, misleading content, or alteration of original artifacts

Bias and Discrimination

Production of ideologically and/or partisan biased information, or information that are incomplete or contradictory

Recreating Specific Individuals

Generation of images of specific people without their explicit permission, or images of minors

Copyrighted Materials

Obtaining access to or unlawfully using copyrighted materials

USDA Generative AI Acceptable Use Guidelines: **Compliance and Monitoring**

Adherence to Policies

Users must follow cybersecurity, privacy, data, and IT governance policies throughout the AI lifecycle.

System Specific Policies

Users must adhere to all AI service and system policies.

No Expectation of Privacy

Departmental systems are continually monitored.

Cybersecurity Incidents

Users must report suspected data spillage, compromise, or inappropriate use of Generative AI tools.

USDA United States Department of Agriculture
Animal and Plant Health Inspection Service

What's happening with AI in PPQ

Staff assisting with USDA testing of M365 Copilot and Copilot for GitHub

Decision on licensing options expected Oct 2025

M365 Copilot very popular for increasing productivity

Rapid adoption of vibe coding, positive impact on productivity

Free, limited version of GitHub Copilot available to staff in VS Code IDE

No USDA approved options for using LLMs yet (except for Copilot testing)

Access to major AI websites is blocked, including documentation and knowledge resources

What’s happening with AI in PPQ

Relying heavily on external collaborators – researchers and commercial vendors – to evaluate appropriate Generative AI use cases within their secure networks

External collaborators also playing critical role in helping staff learn skills and adopt new technologies

Highest value use case currently is data creation from document libraries, expect this to accelerate approved solution for LLM

Thank you