carahsoft

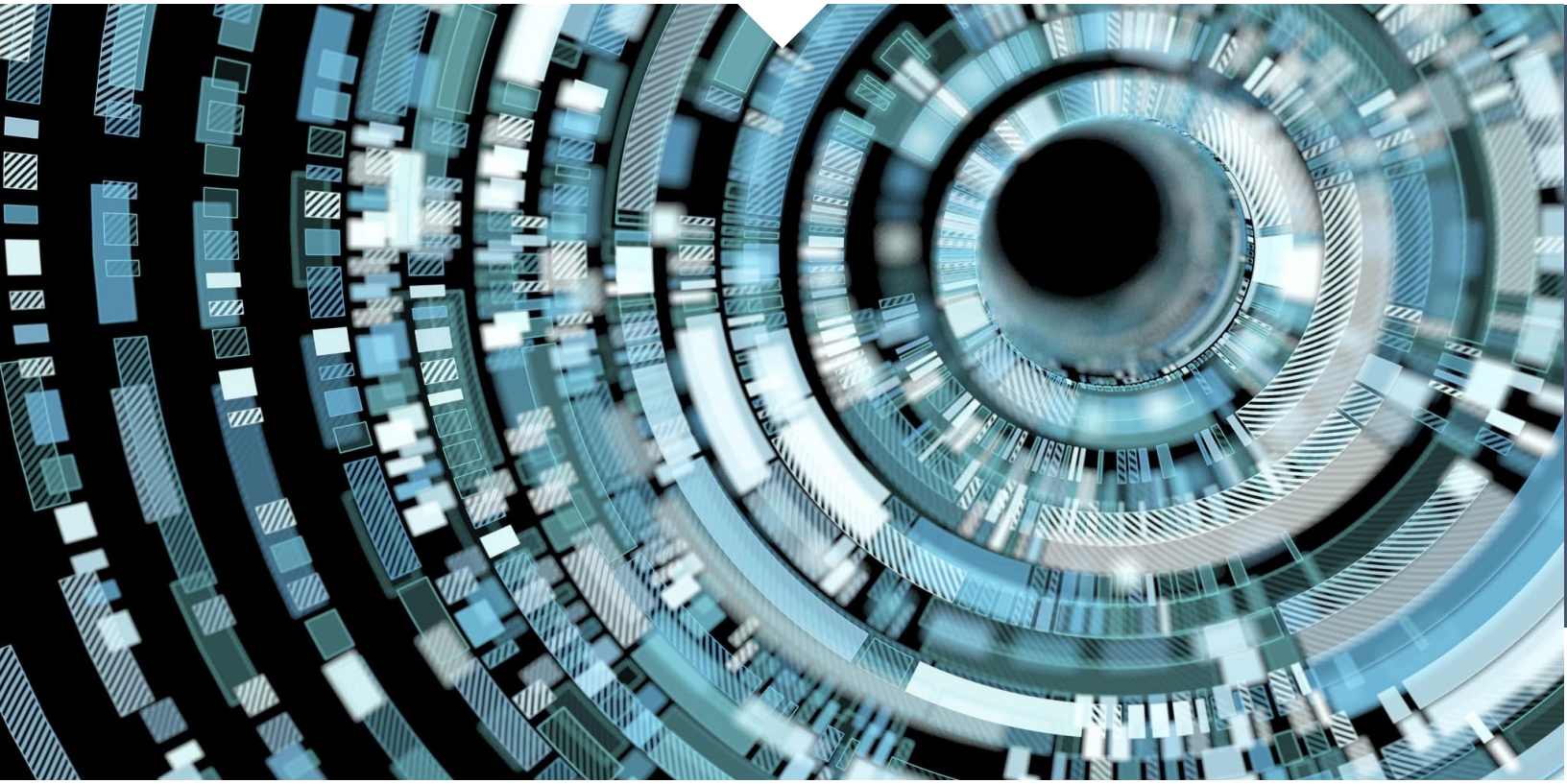
Technology by Policy

ARTIFICIAL INTELLIGENCE

OMB M-25-21

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

April 7, 2025



© 2025 Carahsoft Technology Corp. Proprietary & Confidential

Table of Contents:

Executive Summary	3
How M-25-21 Differs from M-24-10	3
Agency AI Strategies	3
Agency AI Data and Asset Sharing	4
Effective Federal Procurement of AI	4
Enabling an AI-Ready Federal Workforce	4
Chief AI Office Responsibilities	4
AI Governance Board	5
High Impact AI Definition	6
High Impact AI Waivers	7
High Impact AI Minimum Practices	8
Additional Resources	9
Appendix: Timeline of Actions	9

© 2025 Carahsoft Technology Corp. Proprietary & Confidential

Executive Summary

The Office of Management and Budget (OMB) released M-25-21 *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust* on April 3, 2025. The memo rescinds and replaces M-24-10 *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* issued by the Biden Administration. The memo seeks to "lessen the burden of bureaucratic restrictions and to build effective policies and processes for the timely deployment of AI." The DoD and National Security Systems are exempt from the provisions of this memo.

How M-25-21 Differs from M-24-10

M-25-21 draws heavily from it's predecessor M-24-10, and keeps in place a number of the requirements included in the original memo.

The majority of guidance originally given for "Safety and Rights Impacting AI" laid out in M-24-10 is kept for "High Impact AI" in M-25-21. M-25-21 does not differentiate between AI systems that impact safety versus those that impact civil rights or civil liberties. The number of "presumed" High Impact use cases has been narrowed from M-24-10 with several specific areas consolidated under a more general "access to government benefits" section.

The memo maintains very similar policy to the Biden Administration when it comes to focusing on open source models, protecting government data, avoiding vendor lock-in, enabling the AI workforce (with a larger focus on existing personnel), and the responsibilities of the Chief AI Officer.

Agency AI Strategies

By **December 26, 2025**, every cabinet-level agency must develop an AI strategy "for identifying and removing barriers to their responsible use of AI and for achieving enterprise-wide improvements in the maturity of their application" per Section 2a.

The memo encourages agencies "utilize and scale existing tools, processes, and resources for AI governance" in order to avoid creating additional bureaucracy.

These strategies must include plans or processes to:

- develop AI-enabling infrastructure across the AI lifecycle including development, testing, deployment, continuous monitoring;
- ensure access to quality data for AI and data traceability;
- develop enterprise capacity for AI innovation;
- provide AI tools and capacity to support the agency's AI research and development
- (R&D) efforts;
- develop the necessary operations, governance, and infrastructure to manage risks from the use of AI, including risks related to information security and privacy;

© 2025 Carahsoft Technology Corp. Proprietary & Confidential

- recruit, hire, train, retain, and empower an AI-ready workforce and achieve AI literacy for non-practitioners involved in AI; and
- identify, track, and facilitate future AI investment or procurement.

Agency AI Data and Asset Sharing

Section 2b encourages agencies to share AI code, models, and data government-wide and maintain the code as open source software in a public repository unless restricted from doing so by federal law, national security risks, contractual obligations, or risk to agency mission.

Effective Federal Procurement of AI

Section 2d recommends agencies treat data improvements such as cleaning and labeling as a "critical asset" for AI maturity. Agencies should take whatever steps necessary to ensure their contracts retain rights to federal government data through all phases of development and prevent vendor lock-in. Federal data should not be used by vendors to improve their own systems without consent from the agency.

Agencies should track the performance of their models specifically by:

- documenting known capabilities and limitations of the AI and any guidelines on how the system is intended to be used;
- documenting provenance of the data used to train, fine-tune, or operate the AI;
- conducting ongoing testing and validation on AI model performance; the effectiveness of vendor AI offerings; and associated risk management measures, including by testing in real-world conditions;
- assessing for overfitting to known test data, ensuring that AI developers or vendors are not directly relying on the test data to train their AI systems;
- considering contractual terms that prioritize the continuous improvement, performance monitoring, and evaluation of effectiveness of procured AI; and requiring sufficient post-award monitoring and evaluation of effectiveness ofthe AI,
- where appropriate in the context of the product or service acquired

Enabling an AI-Ready Federal Workforce

Section 2e recommends agencies develop technical training and resources to better upskill existing staff, focus recruitment efforts on AI talent with operational experience, and track areas of emerging need for AI talent.

Chief AI Officer Responsibilities

Section 3a requires that agencies designate a Chief AI Officer (CAIO) by **June 30, 2025.** For cabinet-level agencies the CAIO must hold a position at "the Senior Executive Service, Scientific and Professional, or Senior Leader level, or equivalent."

© 2025 Carahsoft Technology Corp. Proprietary & Confidential

Section 3a(i) lists the responsibilities of the Chief AI Officer:

- promote agency-wide responsible AI innovation and adoption in accordance with this memorandum through a governance and oversight process;
- coordinate with other responsible agency officials to ensure that the agency's use of AI complies with applicable law and govemmentwide guidance;
- serve as the senior advisor on AI to the head of the agency and within their agency's executive decision-making forums;
- represent their agency in and collaborate with coordination bodies related to their agency's AI activities, including external forums such as AI-related councils, standard-setting bodies, relevant governance boards, or international bodies;
- maintain the agency's AI Use Case Inventory;
- ensure processes are in place for the agency's high-impact AI use, consistent with Section 4 of this memorandum, by:
    - establishing a process for determining and documenting AI use cases as highimpact;
    - establishing processes to measure, monitor, and evaluate the ongoing
    - performance and effectiveness of the agency's high-impact AI applications;
    - overseeing agency compliance with requirements to manage risks from the use of AI, including those established in this memorandum and in relevant law and policy;
    - establishing a process for an independent review of high-impact use cases before risk acceptance, consistent with Section 4;
    - centrally tracking high-impact use cases and use case determinations;
- advise on the transformation of the agency's workforce into an AI-ready workforce;
- ensure that custom-developed AI code and the data used to develop and test AI are appropriately inventoried, shared, and released in agency code and data repositories, in coordination with their agency's relevant officials;
- provide guidance on AI investments to the agency head and agency CFO related to resourcing requirements necessary to implement this memorandum; and
- support agency efforts to track AI spending.

AI Governance Board

Section 3a(ii) requires each cabinet-level agency convene a governance-body by **August 12, 2025**. Existing AI governance bodies are allowed to fulfill this requirement.

Section 3b(ii) requires these governance bodies to issue a compliance plan by **December 26, 2025** and every two years after that until 2036.

Section 3b(iii) requires that agencies update their internal policies on IT infrastructure, data, cybersecurity, and privacy to align with M-25-21 by **May 6, 2026**. This section also states that “Agency policies should aim to advance using models that are built with less data, require less compute, and are inherently more explainable, where possible.”

© 2025 Carahsoft Technology Corp. Proprietary & Confidential

Section 3b(iv) requires agencies establish terms of acceptable use of generative AI that allow the technology to be used in the agency without undue risk by **May 6, 2026.**

High-Impact AI Definition

Section 5 of the memo defines High-Impact AI as "AI with an output that serves as a principal basis for decisions or actions with legal, material, binding, or significant effect on:

- an individual or entity's civil rights, civil liberties, or privacy; or
- an individual or entity's access to education, housing, insurance, credit, employment, and other programs;
- an individual or entity's access to critical government resources or services;
- human health and safety;
- critical infrastructure or public safety; or
- strategic assets or resources, including high-value property and information marked as sensitive or classified by the Federal Government.

Section 6 of the memo defines a number of AI use cases that are presumed to be high impact:

- **Critical Infrastructure:** Safety-critical functions of critical infrastructure or government facilities, emergency services, fire and life safety systems within structures, food safety mechanisms, or traffic control systems and other systems controlling physical transit;
- **Robotic Equipment:** Physical movements of robots, robotic appendages, vehicles or craft (whether land, sea, air, or underground), or industrial equipment that have the potential to cause significant injury to humans;
- **Kinetic or Non-Kinetic Attacks:** Use of kinetic or non-kinetic measures for attack or active defense in real world circumstances that could cause significant injury to humans;
- **Hazardous Materials:** Transport, safety, design, development, or use of hazardous chemicals or biological agents;
- **Infrastructure Development:** Design, construction, or testing of equipment, systems, or public infrastructure that would pose a significant risk to safety if they failed;
- **Healthcare Practice & Costs:** In healthcare contexts, the medically relevant functions of medical devices; patient diagnosis, risk assessment, or treatment; the allocation of care in the context of public insurance; or the control of health-insurance costs and underwriting;
- **Access Control:** Control of access to, or the security of, government facilities;
- **Trade Controls:** Adjudication or enforcement of sanctions, trade restrictions, or other controls on exports, investments, or shipping;
- **Speech Protections:** The blocking, removal, hiding, or limitation of the reach of protected speech;
- **Crime Forecasting, Surveillance, and Adjudication:** In law enforcement contexts, production of risk assessments about individuals; identification of criminal suspects; forecast of crime; tracking of non-governmental vehicles over time in public spaces; application of biometric identification

© 2025 Carahsoft Technology Corp. Proprietary & Confidential

(e.g., iris, facial, fingerprint, or gait matching); facial reconstruction based on genetic information; social media monitoring; application of digital forensic techniques; use of cyber intrusions; physical location-monitoring or tracking of individuals; detection of weapons or violent activity; or determinations related to recidivism, sentencing, parole, supervised release, probation, bail, pretrial release, or pretrial detention;

- **Immigration & Asylum Status:** Preparation or adjudication of risk assessments related to foreign nationals seeking temporary or permanent access to the U.S. or its territories including related to immigration, asylum, detention, or travel approval status;
- **Biometrics:** Use of biometric identification for one-to-many identification in publicly accessible
- spaces;
- **Federal Benefits:** Ability to apply for, or adjudication of, requests for critical federal services, processes, and benefits to include loans and access to public housing; determination of continued eligibility for ongoing benefits; the control of access-through biometrics or other means (e.g., signature matching)-to IT systems for accessing services for benefits; detection of fraudulent use or attempted use of government services; adjudication of penalties in the context of government benefits;
- **Federal Employment Terms:** Determination of the terms or conditions of Federal employment, including preemployment screening, reasonable accommodation, pay or promotion, performance management, hiring or termination, or recommending disciplinary action; reassignment of workers to new tasks or teams; or
- **Translation:** Provision of language translation (e.g., foreign translation and audiovisual translation) when responses are legally binding or for an interaction that directly informs an agency decision or action.

High Impact AI Waivers

Section 4 of the memo introduces policy requirements that apply only to High Impact AI. Section 4(a) lists how waivers may be issued for minimum practices associated with High Impact AI.

Implementing Risk Management Practices: By **September 22, 2026**, agencies must report their minimum practices for High Impact AI to OMB. If any use cases are not compliant with these minimum practices it must be discontinued. Pilot programs are exempt from the minimum risk practices if they are limited in scale and duration, certification is centrally tracked, opt out and notice options are provided, and minimum risk practices are applied where available.

Authorizing Waivers from Minimum Practices for High-Impact AI: The CAIO can waive requirements of the section through a written-determination if the system would increase risk to safety or rights or cause “unacceptable impediment” to agency operations by fulfilling minimum risk practices.

Tracking Waivers: These waivers must be centrally tracked, be reassessed if the there are changes to the context in which the AI is used, and be reported to OMB within 30 days of issuing a waiver.

© 2025 Carahsoft Technology Corp. Proprietary & Confidential

Publicly Reporting Waivers: These waivers ust be released publicly with a summary describing it's justification.

High Impact AI Minimum Practices

Section 4 of the memo introduces policy requirements that apply only to High Impact AI. Section 4(b) establishes the minimum practices agencies must implement for High Impact AI.

Conduct Pre-Deployment Testing: Agencies must develop pre-deployment testing of models and establish risk mitigation plans.

Complete AI Impact Assessment: Agencies must complete an AI impact assessment that includes information on the intended purpose for the AI and its expected benefit, the quality and appropriateness of the relevant data and model capability, the potential impacts of using AI, reassessment of scheduling and procedures, related costs analysis, results of independent review, and risk acceptance.

Conduct Ongoing Monitoring for Performance and Potential Adverse Impacts: Agencies must continuously monitor AI systems for unexpected changes or impacts to safety, privacy, civil rights, or civil liberties.

Ensure Adequate Human Training and Assessment: Training should be conducted on a periodic basis and should be specific to the AI system.

Provide Additional Human Oversight, Intervention, and Accountability: Agencies should ensure High Impact AI systems have appropriate fail-safes in place.

Offer Consistent Remedies or Appeals: Affected individuals should have access to a timely human review and remediation process that does not place unnecessary burdens on the individual.

Consult and Incorporate Feedback from End Users and the Public: Agencies must provide an option for end users and the public to submit feedback on the system where available.

© 2025 Carahsoft Technology Corp. Proprietary & Confidential

Additional Resources

- M-25-21 Accelerating Federal Use of AI through Innovation, Governance, and Public Trust
- Executive Order 14179 Removing Barriers to American Leadership in Artificial Intelligence
- Executive Order on Advancing United States Leadership in Artificial Intelligence Infrastructure
- Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence
- M-24-18 Advancing the Responsible Acquisition of Artificial Intelligence in Government
- M-24-10 Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence
- FACT SHEET: Vice President Harris Announces OMB Policy to Advance Governance, Innovation, and Risk Management in Federal Agencies' Use of Artificial Intelligence
- Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence
- FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence
- Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence
- DoD: Data, Analytics, and Artificial Intelligence Adoption Strategy
- Industry Letter on President Biden's Executive Order

Appendix: Timeline of Actions

Deadline	Action
June 30, 2025	• Agencies must designate a Chief AI Officer
August 12, 2025	• Agencies must establish an AI Governance Body
December 26, 2025	• Agencies must establish an AI Strategy • Agency governance bodies must issue a compliance plan for M-25-21
May 6, 2026	• Agencies must update their internal policies on IT infrastructure, data, cybersecurity, and privacy to align with M-25-21 • Agencies must issue acceptable terms of risk for generative AI deployment
September 22, 2026	• Agencies must report their minimum practices for High Impact AI to OMB

© 2025 Carahsoft Technology Corp. Proprietary & Confidential