ML STRATEGIES

OMB Issues Guidance to Federal Agencies on the Use of Artificial Intelligence — AI: The Washington Report

April 09, 2024 | | By **Bruce Sokler**, **Alexander Hecht**, **Christian Tamotsu Fjeld**, Raj Gambhir

1. Pursuant to President Biden's October 2023 **executive order on AI**, in March 2024 the Office of Management and Budget issued a **memorandum** directing the use of AI by federal agencies.
2. Among other provisions, the memorandum directs agencies to designate a Chief AI Officer, create a publicly accessible AI use case inventory, and carry out proper due diligence when procuring AI tools.
3. Most significantly, the memorandum mandates that agencies determine which AI use cases are safety and/or rights-impacting and requires that agencies follow certain minimal practices with regard to these AI uses.**[1]**

On March 28, 2024, the Office of Management and Budget (OMB) released a memorandum on **Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence**. The OMB's memorandum directs agencies to "advance AI governance and innovation while managing risks from the use of AI in the Federal Government, particularly those affecting the rights and safety of the public."

The AI risks this memo addresses are specifically those that "result from any reliance on AI outputs to inform, influence, decide, or execute agency decisions or actions, which could undermine the efficacy, safety, equitableness, fairness, transparency, accountability, appropriateness, or lawfulness of such decisions or action."

Most of the memorandum's requirements apply to "all agencies defined in **44 U.S.C. § 3502(1)**." Some provisions only apply to Chief Financial Officers Act (CFO Act) agencies identified in **31 U.S.C. § 901(b)** and other requirements don't apply to members of the intelligence community as defined in **50 U.S.C. § 3003**.

It is important to note that AI deployed as part of a component of a National Security System is not subject to the requirements of this memorandum. Such AI is to instead be regulated by other policies and practices developed by the DOD and related agencies.

The memorandum's requirements fall into four broad categories:

1. **Strengthening Artificial Intelligence Governance**
2. **Advancing Responsible Artificial Intelligence Innovation**
3. **Managing Risks from the Use of Artificial Intelligence**
4. **Managing Risks in Federal Procurement of Artificial Intelligence**

Strengthening Artificial Intelligence Governance

- **Designating Chief AI Officers (CAIO)**: By May 27, 2024, the head of each agency must designate a CAIO. Each CAIO will be tasked with managing their agency's AI operations, ensuring compliance with applicable government mandates related to AI, coordinating with other agencies about AI matters, and

more. A CAIO must have the requisite knowledge to execute these responsibilities. Agencies may choose to designate an existing executive (e.g. Chief Technology Officer, or Chief Information Officer) to be their CAIO.

- **Convening Agency AI Governance Bodies**: By May 27, 2024, each CFO Act agency must "convene its relevant senior officials to coordinate and govern issues tied to the use of AI within the Federal Government." These meetings must take place on at least a semi-annual basis.
- **Compliance Plans**: By September 24, 2024, and then every two years thereafter until 2036, each agency must make publicly available either a document detailing their plans to comply with the memo or a determination that they do not nor plan to use covered AI.
- **AI Use Case Inventories**: Every agency (except the DOD and the intelligence community) must inventory each of its AI use cases at least annually, submitting this inventory to both the OMB and its website. Agencies will be required to identify which use cases are "safety-impacting and rights-impacting AI and report additional detail on the risks—including risks of inequitable outcomes—that such uses pose and how agencies are managing those risks."
- **Reporting on AI Use Cases Not Subject to Inventory**: Those applicable AI use cases that are not required to be individually inventoried (such as those pertaining to the DOD and intelligence community) must nevertheless be reported to the OMB, but in an aggregate fashion.

Advancing Responsible Artificial Intelligence Innovation

- **Charting AI Strategy**: By March 28, 2025, each CFO Act agency must make publicly available a strategy for "identifying and removing barriers to the responsible use of AI and achieving enterprise-wide improvements in AI maturity." This strategy must include details such as the agency's planned uses of AI that are most impactful to its mission, an assessment of the agency's current AI maturity, and an assessment of the agency's AI workforce needs.
- **Removing Barriers to the Responsible Use of AI**: Agencies should ensure that their AI projects have "access to adequate IT infrastructure," sufficient data to operate, robust cybersecurity protections and be subject to appropriate oversight measures.
- **Fostering AI Talent**: Agencies are directed to designate an AI Talent Lead responsible for reporting to agency leadership on AI talent acquisition, provide "Federal employees pathways to AI occupations and that assist employees affected by the application of AI to their work," and develop internal AI talent.
- **Facilitating AI Sharing and Collaboration**: Except in certain cases, agencies are directed to make their AI models and model weights open source. Where portions of an AI project's code are not able to be shared, the agency should share the rest of the project's code "where practicable".
- **Harmonizing Artificial Intelligence Requirements**: OMB and the Office of Science and Technology Policy will, through an interagency council, "will coordinate the development and use of AI in agencies' programs and operations" across the federal government.

Managing Risks from the Use of Artificial Intelligence

- **Determining Which Artificial Intelligence Is Presumed to Be Safety-Impacting or Rights-Impacting**: Agencies, excepting those that are elements of the intelligence community, must review each current or planned use of AI to assess whether it matches the definition of safety-impacting AI or rights-impacting AI. For every AI use determined to be safety-impacting or rights-impacting, by December 1, 2024 agencies must cease the AI use, obtain a one year extension from OMB to continue the use, secure a waiver on the practice from OMB, or implement certain "minimum practices."

Rights-Impacting AI:	Safety-Impacting AI:

The term “rights-impacting AI” refers to AI whose output serves as a principal basis for a decision or action concerning a specific individual or entity that has a legal, material, binding, or similarly significant effect on that individual’s or entity’s:

1. Civil rights, civil liberties, or privacy, including but not limited to freedom of speech, voting, human autonomy, and protections from discrimination, excessive punishment, and unlawful surveillance;

2. Equal opportunities, including equitable access to education, housing, insurance, credit, employment, and other programs where civil rights and equal opportunity protections apply; or

3. Access to or the ability to apply for critical government resources or services, including healthcare, financial services, public housing, social services, transportation, and essential goods and services.

The term “safety-impacting AI” refers to AI whose output produces an action or serves as a principal basis for a decision that has the potential to significantly impact the safety of:

1. Human life or well-being, including loss of life, serious injury, bodily harm, biological or chemical harms, occupational hazards, harassment or abuse, or mental health, including both individual and community aspects of these harms;

2. Climate or environment, including irreversible or significant environmental damage;

3. Critical infrastructure, including the critical infrastructure sectors defined in Presidential Policy Directive 21 or any successor directive and the infrastructure for voting and protecting the integrity of elections; or,

4. Strategic assets or resources, including high-value property and information marked as sensitive or classified by the Federal Government.

  - *Minimum practices **prior** to adopting a safety of rights-impacting AI use case*: Conducting an AI impact assessment for the use case in question, testing the AI use case for performance in a real-world context, and independently evaluating the AI.
  - *Minimum practices **after** adopting a safety of rights-impacting AI use case*: Conducting ongoing monitoring, regularly evaluating risks from the use of AI, mitigating emerging risks to rights and safety, ensuring adequate human training and assessment. And providing public notice and plain-language documentation of the AI use case. Agencies must also commit to providing “additional human oversight, intervention, and accountability as part of decisions or actions that could result in a significant impact on rights or safety.”
  - *Additional minimum practices **before** adopting rights-impacting AI*: Identifying and assessing the AI’s impact on equity and fairness, mitigating algorithmic discrimination when present, consulting and incorporating feedback from affected communities and the public.
  - *Additional minimum practices **before** adopting rights-impacting AI*: Conducting ongoing monitoring and mitigation for AI-enabled discrimination, notifying negatively affected individuals, maintaining human consideration and remedy processes, creating options to opt-out of AI-enabled decisions.

Managing Risks in Federal Procurement of Artificial Intelligence

- **Ensuring Legal Compliance**: Ensuring that AI is procured in a manner that is legal and conforms to all relevant regulation.
- **Performing Due Diligence**: Obtaining adequate documentation on the capabilities and limitations of the AI tools being procured. Considering “contracting provisions that incentivize the continuous improvement of procured AI” and “requiring sufficient post-award monitoring of the AI, where appropriate in the context of the product or service acquired.”
- **Promoting Competition in the Procurement of AI**: “Agencies should take appropriate steps to ensure that Federal AI procurement practices promote opportunities for competition among contractors and do not improperly entrench incumbents.”
- **Maximizing the Value of Data for AI**: “Agencies should take steps to ensure that their contracts retain for the Government sufficient rights to data and any improvements to that data so as to avoid vendor lock-in and facilitate the Government’s continued design, development, testing, and operation of AI.”
- **Overfitting to Known Test Data**: “When testing AI using data that its developer may have access to…agencies should ensure, as appropriate, that their AI developers or vendors are not directly relying on the test data to train their AI systems.”
- **Responsible Procurement of AI for Biometric Identification**: When procuring AI systems that identify individuals using biometric identifiers, agencies are encouraged to address the risk that data used to train the model may not be lawfully collected or else be insufficiently accurate, and request

supporting documentation or test results to validate the accuracy of the model.
- **Responsibly Procure Generative AI**: “Agencies are encouraged to include risk management requirements in contracts for generative AI.”
- **Assessing for Environmental Efficiency and Sustainability**: Agencies should consider the environmental impact of procuring computationally intensive AI services.

We will continue to monitor, analyze, and issue reports on these developments. Please feel free to contact us if you have questions as to current practices or how to proceed.

Endnotes

---

[1] This requirement is subject to certain limitations, which are discussed in greater length in this newsletter and the **text of the memorandum**.

Authors

Bruce Sokler

Bruce D. Sokler is a Mintz antitrust attorney. His antitrust experience includes litigation, class actions, government merger reviews and investigations, and cartel-related issues. Bruce focuses on the health care, communications, and retail industries, from start-ups to Fortune 100 companies.

Alexander Hecht, Executive Vice President & Director of Operations

Alexander Hecht is Executive Vice President & Director of Operations of ML Strategies, Washington, DC. He's an attorney with over a decade of senior-level experience in Congress and trade associations. Alex helps clients with regulatory and legislative issues, including health care and technology.

Christian Tamotsu Fjeld, Senior Vice President

Christian Tamotsu Fjeld is a Vice President of ML Strategies in the firm’s Washington, DC office. He assists a variety of clients in their interactions with the federal government.

Raj Gambhir

Raj Gambhir is a Project Analyst in Washington, DC.