CLIENT ALERTS & INSIGHTS

Government-Wide Policy Provides Federal Agencies Governance Structure and Standards for Use of Artificial Intelligence

MAY 2, 2024

Authors: Megan C. Parker, Kristopher J. Chandler

Marking the first effort to establish an artificial intelligence ("AI") governance structure for the federal government, the AI Memorandum contains requirements and recommendations for federal agencies' AI use that private-sector companies should pay attention to in implementing their own AI risk management and acceptable use policies.

In March 2024, the Office of Management and Budget ("**OMB**") issued its first government-wide policy as memorandum M-24-10 titled "Advanced Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence" (the "**AI Memorandum"**).

Pursuant to President Biden's October 2023 AI Executive Order, the AI Memorandum directs federal agencies to "advance AI governance and innovation while managing risks from he use of AI in the Federal Government, particularly those affecting the rights and safety of the public."

Scope

The risks addressed specifically are those that "result from any reliance on AI outputs to inform, influence, decide, or executive 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 AI Memorandum applies to "all agencies defined in 44 U.S.C. § 3502(1)" while other provisions only apply to agencies identified in the Chief Financial Officers Act ("**CFO Act**") (31 U.S.C. § 901(b)). Certain requirements do not apply to members of the intelligence community as defined in 50 U.S.C § 3003.

Further, system functionality that "implements or is reliant on" AI that is "developed, used or procured by" the covered agencies is subject to the AI Memorandum. Activity merely relating to AI, including regulatory actions for nonagency AI use or investigations of AI in an enforcement action, and AI deployed as part of a component of a National Security System are not covered.

Specifically, the AI Memorandum's requirements and recommendations fall into four categories: (1) strengthening AI governance, (2) advancing responsible AI Innovation, (3) managing risks from use of AI, and (4) managing risks in federal procurement of AI.

Strengthening AI Governance

By May 27, 2024, each agency must designate a Chief AI Officer ("**CAIO**") who will "bear the primary responsibility . . . for implementing the memorandum" by managing the agency's AI operations, ensuring compliance with AI-related government mandates, coordinate with other agencies on AI, and more. More than 15 agencies, the first having been the Department of Homeland Security on Oct. 30, 2023, have designated a CAIO to date.

Next, agencies covered by the CFO Act must convene "its relevant senior officials to coordinate and govern issues tied to use of AI within the Federal Government[,]" or AI governance bodies, by May 27, 2024, and meet at least semi-annually.

Third, every agency (excluding the Department of Defense ("**DOD**") and the intelligence community) must inventory each of its AI use cases at least annually, submitting each inventory to the OMB and the AI Use Inventory website. The inventory must identify which use cases are "safety-impacting and rights-impacting and report additional detail on the risks-including risks of inequitable outcomes-that such uses pose and how agencies are managing those risks. The OMB published draft guidance on this reporting requirement.

For AI use cases not required to be individually inventoried, such as those of the DOD and intelligence community, the AI Memorandum requires those to still be reported to the OMB in an aggregate fashion.

Lastly, by Sept. 24, 2024, and every two years thereafter until 2036, each agency must make publicly available either a document detailing their plans to comply with the AI Memorandum or a determination that they do not nor plan to use AI as covered.

Advancing Responsible AI Innovation

First, 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." Agencies must include various details such as its planned uses of AI that are most impactful to its mission, an assessment of its current AI maturity, and assessment of its AI workforce needs.

Next, agencies are directed to ensure their AI projects have "access to adequate IT infrastructure," sufficient data to operate, robust cybersecurity protection, and appropriate oversight measures. Meanwhile, the AI Memorandum also directs agencies to make their AI code and models open source where practicable.

Third, the AI Memorandum recommends that agencies designate an AI Talent Lead who "will be accountable for reporting . . . AI hiring across the agency" as part of providing "Federal employees pathways to AI occupations" and assisting "employees affected by the application of AI to their work[.]"

Lastly, the OMB will collaborate with the Office of Science and Technology Policy to coordinate agencies' development and use of AI by promoting shared templates and formats, sharing best practices and technical resources, and highlighting exemplary uses of AI.

Managing Risks from Use of AI

By Dec. 1, 2024, agencies (excluding those of the intelligence community) will be required to implement concrete safeguards when using safety-impacting or rights-impacting AI. If agencies cannot apply the required safeguards, the agency must cease using the AI system unless it can justify why non-use would increase risks to safety or rights or create an unacceptable impediment.



As part of implementing the safeguards, the AI Memorandum provides several practices agencies must implement prior and after adopting a safety or rights-impacting AI tool.

At minimum prior to adoption, an agency must conduct an AI impact assessment for each use case in question, test each AI use case for performance in a real-world context, and independently evaluate the AI system.

Additional practices prior to adoption the AI Memorandum recommends include identifying and assessing the AI's impact on equity and fairness, conducting ongoing monitoring and mitigation for AI-enabled discrimination, and creating options to opt-out of AI-enabled decisions.

Then, at minimum after adoption with the safeguards in place, agencies must conduct ongoing monitoring to regularly evaluate risks from use of the AI, ensure adequate human training and assessment, mitigate emerging risks to rights and safety, and provide public notice and plain-language documentation of AI use cases.

The AI Memorandum also requires agencies commit to providing "additional human oversight, intervention, and accountability as part of decisions or actions that could result in significant impact on rights or safety."

Managing Risks in Federal Procurement of AI

In addition to directing AI to be procured in a legal manner that conforms to all relevant regulation, the AI Memorandum directs agencies to obtain adequate documentation on the AI's capabilities and limitations. Additionally, agencies should consider "contracting provisions that incentivize the continuous improvement" and post-procurement monitoring of the AI system.

Similarly, the AI Memorandum encourages agencies "to include risk management requirements in contracts for generative AI."

In relation to the data aspect of AI, the AI Memorandum directs agencies "to ensure that their contracts retain for the Government sufficient rights to data and any improvements" while ensuring that any test data used to assess an AI system is not being used to further train the AI system.

Lastly, the AI Memorandum places additional emphasis on agencies addressing risks when using AI systems that identify individuals through biometric identifiers, such as any risk that data used to train the model was not lawfully collected or is insufficiently accurate, and request documentation validating the AI system's accuracy.

Conclusion

Although the AI Memorandum explicitly addresses federal agency use of AI and does not extend to the private sector, history shows that federal government use and guidance impact the development of best practices adopted by companies. As such, private sector companies using AI should evaluate and consider how their current AI practices and policies align with the AI Memorandum and future guidance on the federal government's use of AI.

Evaluating and considering how an organization's current AI practices and policies align with the AI Memorandum and future guidance will require careful assessment. The Benesch AI Commission is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts or questions involving safe implementation of AI.

Megan C. Parker at mparker@beneschlaw.com or 216.363.4416.

Kristopher J. Chandler at kchandler@beneschlaw.com or 614.223.9377.