APRIL 9, 2024

OMB Releases Policy to Advance Governance, Innovation, and Risk Management for Federal Agency Use of Artificial Intelligence

by Tatum Andres , Stephen M. Anstey , John C. F. Loving

In today's rapidly evolving technological landscape, artificial intelligence ("AI"), and particularly generative AI, continues to develop as a powerful tool not only for industry but also government entities. The successful integration of AI within vast federal government systems necessitates meticulous planning and robust governance frameworks. The Office of Management and Budget ("OMB") plays a pivotal role in ensuring effective management of governmental programs and resources. Among its responsibilities is the supervision of agency utilization of AI technology. To support the federal government in its efforts to responsibly leverage the opportunities AI presents, OMB released its first governmentwide AI policy.

The OMB policy, which was published on March 28, 2024, was provided as a memorandum for the Heads of Executive Departments and Agencies titled *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence*. OMB also published related draft guidance concerning agency reporting requirements regarding federal government AI use. The policy notes that by December 1, 2024, federal agencies will be expected to implement safeguards to assess, test, and monitor the impact of artificial intelligence on the public. According to the accompanying Fact Sheet published by the White House, the new policy requires federal agencies to increase transparency over the use of AI, and remove "unnecessary barriers to AI innovation," while also actively "encourage[ing] agencies to responsibly experiment with generative AI."

Strengthening Artificial Intelligence Governance

The policy issued mandates several critical measures to enhance the responsible implementation of AI across federal agencies. First, it necessitates that each federal agency appoint a Chief AI Officer ("CAIO") within a tight timeframe of 60 days. This CAIO will collaborate with other designated officials to streamline agency AI utilization, foster innovation in AI technologies, and effectively mitigate associated risks. However, the CAIO will not be working alone. Under the policy, agencies are also required to establish an AI Governance Board to convene relevant senior officials to govern agency use of AI. The AI Governance Boards must be chaired by the Deputy Secretary of the agency or equivalent and vice-chaired by the agency CAIO. The full Board, including the Deputy Secretary, must convene on at

least a semi-annual basis.

Among other things, the AI Governance Board is responsible for the removal of barriers to the use of AI. Agencies are encouraged to have their AI Governance Boards consult with external experts to help broaden the perspective of an existing governance board and inject additional technical, ethics, civil rights, civil liberties, and sector-specific expertise. Additionally, consistent with Section 10.2 of Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence ("EO on AI") agencies are strongly encouraged to prioritize recruiting, hiring, developing, and retaining talent in AI and AI-enabling roles to increase enterprise capacity for responsible AI innovation.

This directive underscores the critical importance of bolstering federal workforce expertise and proficiency in AI technologies, thereby enhancing the overall organizational capacity for fostering responsible AI innovation. By prioritizing the cultivation of a skilled workforce adept in AI and its enabling technologies, agencies can effectively promote the development of AI applications that serve the public interest. This strategic approach intends to amplify an agency's ability to harness the potential of AI while also reinforcing its commitment to advancing innovation in a manner that upholds principles of accountability, transparency, and fairness.

Advancing Responsible Artificial Intelligence Innovation

The policy delineates specific categories of AI presumed to have an impact on society and outlines minimum standards and practices for the utilization of AI, particularly in contexts where safety and rights are impacted. Agencies must apply the defined minimum risk management practices to safety-impacting and rights-impacting AI by December 1, 2024, or stop using relevant AI systems until they achieve compliance (unless agency leadership justifies why ceasing to use the AI system increases risks to safety or rights overall or would create an unacceptable impediment to critical agency operations).

Per the policy, 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 2159 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

The policy also defines "rights-impacting AI", which 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.

To strike a delicate balance between fostering progress and upholding fundamental values of fairness, each agency must develop and release publicly on the agency's website a strategy for identifying and removing barriers to the responsible use of AI and achieving enterprise-wide improvements in AI maturity within 365 days of the issuance of the policy.

Additionally, within 180 days of the issuance of the policy, and thereafter every two years until 2036, each agency is required to submit to OMB and publicly disclose on the agency's website, either a strategy outlining steps to align with the directives denoted in the memorandum or a formal declaration stating that the agency neither employs nor foresees the use of AI technologies covered by the directive. If the agency uses AI technology, the policy states that each agency must individually inventory each of its AI use cases at least annually.

The policy makes clear that transparent utilization of AI is a central goal of the White House. To assist in this effort, OMB, in collaboration with the Office of Science and Technology Policy ("OSTP"), will coordinate the development and use of AI in agency programs and operations—including the implementation of this memorandum—across Federal agencies through an interagency council. These efforts will include:

1. Promoting shared templates and formats;
2. Sharing best practices and lessons learned, including for achieving meaningful participation from affected communities and the public in AI development and procurement, updating organizational processes to better accommodate AI, removing barriers to responsible AI innovation, responding to AI incidents that may have resulted in harm to an individual, and building a diverse AI workforce to meet the agency's needs;
3. Sharing technical resources for implementation of the memorandum's risk management practices, such as for testing, continuous monitoring, and evaluation; and
4. Highlighting exemplary uses of AI.

Managing Risks from the Use of Artificial Intelligence

Ensuring the responsible integration of AI into agency operations requires proactive risk assessment. The policy mandates that agencies, thorough testing, ensure that AI systems, along with their associated components, perform effectively within their intended real-world applications. Additionally, the policy requires an independent evaluation of AI systems to verify their proper functioning and alignment with intended objectives, in order to ensure that the anticipated benefits outweigh potential risks. Notably, the independent reviewing authority must not have participated directly in the system's development, although OMB does not specify that this authority must be external to the agency itself.

Furthermore, federal agencies are instructed to implement continuous monitoring mechanisms to detect any deterioration in the functionality of AI systems and to identify changes in their impact on rights and safety. The policy underscores the importance of conducting an annual "human review" to assess whether AI related deployment context, associated risks, benefits, and agency requirements have evolved over time. This human review process must include testing and oversight by an appropriate internal agency authority not directly involved in the system's development or operation.

Notably, the policy provides an entire section on the responsible procurement of AI for biometric identification, including the use of biometric identification by law enforcement and in publicly accessible spaces. Specifically, the policy states that when procuring systems which use AI to identify individuals using biometric identifiers—e.g., faces, irises, fingerprints, or gait—agencies are encouraged to

1. Assess and address the risks that the data used to train or operate the AI may not be lawfully collected or used, or else may not be sufficiently accurate to support reliable biometric identification. This includes the risks that the biometric information was collected without appropriate consent, was originally collected for another purpose, embeds unwanted bias, or was collected without validation of the included identities; and
2. Request supporting documentation or test results to validate the accuracy, reliability, and validity of the AI's ability to match identities.

Although OMB's conclusive guidance explicitly addresses federal agency internal utilization of AI and stipulates that it does not extend to the private sector, precedent indicates that federal government uses and guidance will impact the development of "best practices" for industry use, including AI risk management and compliance. At a minimum, private sector companies using AI should evaluate and consider how their current AI practices align with OMB's guidance and requirements for the federal government's own use of AI.

Kilpatrick

Kilpatrick – Generative AI

Kilpatrick's Generative AI practice works with clients to tackle their most pressing AI concerns and challenges to achieve results in line with overall business strategies and goals. Our multidisciplinary

team, with backgrounds in intellectual property, privacy, cybersecurity, federal legislation and regulation, energy, commercial transactions, and dispute resolution, monitors and proactively addresses risks, compliance requirements, and opportunities related to generative AI. For more information, please visit our website: Kilpatrick – Generative AI

Kilpatrick – Government and Regulatory

Kilpatrick's Government and Regulatory practice offers policy, legislative, rulemaking, compliance, and regulatory advocacy services and legal guidance on both broad and industry-specific matters, including artificial intelligence, energy, sustainability, Tribal, finance, distributed ledger technology (including blockchain), and digital assets (cryptocurrency, stablecoin, tokenization, and central bank digital currency (CBDC)). For more information, please visit our website: Kilpatrick – Government & Regulatory