HIMSS

Fact Sheet: Governance Framework for Agency Use of Artificial Intelligence Memo

United States Office of Management and Budget: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence

Artificial Intelligence Use in Agencies

White House: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence (pdf)

Key Takeaways

- The guidance establishes a definition for covered AI as well as required mechanisms and processes federal agencies must utilize to deploy AI that meets the definition.
- The guidance from the Office of Management and Budget (OMB) establishes requirements for U.S. federal agencies to have an appropriate governance structure, including the hiring of an AI CIO by the head of each agency, testing and field-testing requirements, validating safe manufacturing practices prior to selection of AI tools and monitoring of AI performance consistent with expected outcomes.
- The guidance lacks a mandated revalidation timeline or framework but vaguely establishes requirements for monitoring AI performance.
- AI must meet the minimum practices requirements or be shut down after Dec. 1, 2024.
- AI must be revalidated, at a minimum, annually after Dec. 1, 2024.

Defining "Covered AI"

- Incorporates the definition used in Section 238(g) of the John S. McCain National Defense Authorization Act of 2019
- Covered AI includes:
    - Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight or that can learn from experience and improve performance when exposed to data sets.
    - An artificial system developed in computer software, physical hardware or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication or physical action.
    - An artificial system designed to think or act like a human, including cognitive architectures and neural networks.

  - A set of techniques, including machine learning, that is designed to approximate a cognitive task.
  - An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making and acting.
- The definition includes machine learning deep learning, reinforcement learning, transfer learning and generative AI.
- The definition does not include robotic process automation/systems whose behavior is defined only by human-defined rules or that learn solely by repeating an observed practice exactly as it was conducted.
- No system should be considered too lacking in technical complexity (too few parameters) to qualify as covered AI.

Governance

- By June 1, 2024, heads of federal agencies must select an agency chief AI officer (CAIO).
- By June 1, 2024, heads of federal agencies must name and convene key stakeholders to form agency-wide AI governance bodies which will "coordinate and govern" issues associated with AI and the agency.
- By Sept. 1, 2024, each agency must submit to OMB and post publicly on the agency website its governance plan, consistent with the requirements in the memorandum using OMB provided templates.
- Agencies (with Department of Defense and the Intelligence Community exempted) will be required to inventory AI use cases.
- As part of the inventory process, agencies will be required to identify which use cases are "safety-impacting" and "rights-impacting AI" including risks of inequitable outcomes, reporting the inventory to OMB.

Pre-Deployment Requirements

- By Dec. 1, 2024, agencies must utilize the following minimum practices or discontinue use of any AI that doesn't meet the minimum practices requirements.
- Minimum practice requirements:
  - Complete an AI Impact Assessment
    - Measure assessment of Intended Purpose and Expected Benefit of AI
    - Potential risks (including an assessment of what specific steps an agency needs to take where risks are not mitigated by minimum practice requirements)
    - Quality and appropriateness of data feeding the AI
  - Test models in a real-world environment before deployment, following domain specific best practices.
  - Conduct independent assessments of AI testing performance data, coordinated by the CAIO or AI agency oversight board.
- Exemptions:

    - Use of AI solely to evaluate a potential vendor, commercial capability or freely available AI for the purpose of making a procurement or acquisition decision
    - Use of AI exclusively in controlled testing conditions to carry out the minimum testing requirements
- Extensions can be granted for one year but must be submitted by Oct. 15, 2024, and include justification and strategies for minimizing risk of non-compliance.

Post Deployment Monitoring

- By Dec. 1, 2024, agencies must:
    - Conduct ongoing monitoring of degradation of the AI's functionality to detect changes in the AI's impact on rights and safety.
    - Scale up the use of new or updated AI features incrementally where possible to provide adequate time to monitor for adverse performance or outcomes.
    - Monitor and defend the AI from AI-specific exploits that would adversely impact rights and safety.
    - Regularly evaluate risks from the use of AI.
        - Must include periodic human reviews to determine whether the deployment context, risks, benefits and agency needs have evolved
    - Regularly assess whether the current required minimum practices adequately mitigates new and existing risks
    - Conduct human review of all qualifying AI tools on, at minimum, an annual basis.
- Reviews must also include oversight and consideration by an appropriate internal agency authority not directly involved in the system's development or operation.
- If a risk to rights or safety is identified through the ongoing and periodic monitoring process, agencies must mitigate those risks (including updating the AI to reduce its risks or implementing procedural or stringent human interventions.
- If risks exceed an acceptable level, the agency must stop using the AI mechanism.