Federal Artificial Intelligence (AI) Action Plan Recommendations

Kiri L. Wagstaff, Ph.D.

Thank you for the opportunity to provide input for the new federal Artificial Intelligence (AI) Action Plan. I am an artificial intelligence researcher and educator with a Ph.D. in Computer Science. I have over two decades of experience at the NASA Jet Propulsion Laboratory applying machine learning and artificial intelligence for the benefit of science and society, and I am an elected Fellow of the Association for the Advancement of Artificial Intelligence (AAAI). I have also served the federal government as an AI subject matter expert in policy and legislation.

To advance the administration's AI goals, two critical elements to include in the AI Action plan are steps to (1) increase public AI literacy and (2) ensure deployed AI systems maintain their advertised performance and behavior.

1. Increase Public AI Literacy

AI technology is being used in progressively more aspects of our daily lives, from chatbots to meeting transcription to decision making like loan approvals and criminal sentencing. Lack of public familiarity and confidence in this technology creates barriers to its adoption and responsible use. In a recent survey of 4,800 adults, on average the respondents were only able to correctly assess 3 of 8 statements about AI capabilities,[1] revealing potentially dangerous misconceptions. Lawyers have submitted false information to the court, apparently due to their ignorance of the limitations of a generative AI chatbot.[2] Businesses have likewise deployed AI in inappropriate settings, resulting in misinformation for users and embarrassment and/or fines for the business. Recent examples include Air Canada's chatbot that fabricated a false bereavement policy,[3] PayPal's AI Assistant that fabricated false transactions,[4] and Apple Intelligence that fabricated false news.[5]

Lack of AI literacy leaves us vulnerable to graver mistakes. A journalist could put the lives of their sources at risk by using an AI interview transcription tool without knowing that it could leak confidential information. Patients could make life-threatening mistakes with medication or treatments based on AI-generated advice from a web search.

---

[1] Ognyanova, K. and Singh, V., National AI Opinion Monitor: AI Trust and Knowledge in America (2025), https://naiom.net/public-reports/NAIOM Report 02 AI Trust Knowledge.pdf

[2] Milmo, D. Two US Lawyers Fined for Submitting Fake Court Citations from ChatGPT, *The Guardian* (2023), https://www.theguardian.com/technology/2023/jun/23/two-us-lawyers-fined-submitting-fake-court-citations-chatgpt

[3] Belanger, A., Air Canada Has to Honor a Refund Policy Its Chatbot Made Up, *Wired* (2024), https://www.wired.com/story/air-canada-chatbot-refund-policy/

[4] Anonymous, Incident Number 748: Erroneous Declined Transaction Notification by PayPal AI Assistant, *Artificial Intelligence Incident Database* (2024), https://incidentdatabase.ai/cite/748/

[5] Kleinman, Z., McMahon, L., and Sherman, N. Apple Urged to Withdraw 'Out of Control' AI News Alerts, *BBC* (2025), https://www.bbc.com/news/articles/cge93de21n0o

The U.S. public urgently needs guidance on how to safely and effectively make use of AI products and services. The public does not need to know the internal details of each AI algorithm. What they need is a set of best practices for their use of AI systems.

To promote human flourishing and economic competitiveness by increasing public AI literacy, the AI Action Plan should:

1. Develop a **national strategy for increasing public AI literacy** informed by expertise from government, public, and private organizations.
2. Create guidance on **best practices for specific AI use cases**, such as classification, voice dictation, product recommendation, and content generation (including interactions with AI chatbots), in everyday domains such as personal finance, healthcare, communication, and business operations. This guidance should include topics such as data privacy, the difference between a search engine and a generative model, and the known strengths and limitations of AI models. It should also include key questions to ask before interacting with an AI system, such as
    - "What kind of data was this system trained on?"
    - "What data will be collected about me?"
    - "How long will my data be retained, and how will it be used?"
    - "How well has this system performed in the past?"
3. Conduct a **national media campaign** to disseminate this guidance for the safe and beneficial use of AI products and services. The campaign should maximize its reach by developing messaging in multiple languages and multiple venues (Internet, radio, TV, newspapers, magazines, etc.).

These steps will empower the public to make informed choices about when and how to make use of AI in their lives. Supporters of this approach include IBM,[6] BSA | The Software Alliance,[7] and the AARP.[8]

2. Monitor and Maintain Deployed AI System Performance

The expected performance of a trained AI system is achieved in new settings only when the new data is sufficiently similar to the training data. Applying a trained system or model to new cases or situations creates risk: if the new data differs from the training cases, accuracy and reliability generally go down, often by unpredictable amounts. This concern has been highlighted for clinical healthcare, among other areas: "ML [machine learning] models that do not generalize may fail silently, i.e. perform significantly worse on new samples or individuals unnoticed, especially if not externally validated".[9]

---

[6] Cruz, I.F., AI Literacy: A Prerequisite for the Future of AI and Automation in Government, Ch. 7 (2024), https://www.businessofgovernment.org/sites/default/files/Chapter 7 - AI Literacy Cruz.pdf

[7] Ciccanti, J., BSA SVP Government Relations Craig Albright Comments on AI Literacy Bill (2024), https://www.bsa.org/news-events/media/bsa-svp-government-relations-craig-albright-comments-on-ai-literacy-bill

[8] Sweeney, B. AARP Letter in Support of the Consumers LEARN AI Act (2024), https://www.aarp.org/content/dam/aarp/politics/advocacy/2024/07/consumers-learn-ai-act.pdf

[9] Goetz, L. et al., Generalization—A Key Challenge for Responsible AI in Patient-Facing Clinical Applications, *npj Digital Medicine* 7, 126 (2024), https://doi.org/10.1038/s41746-024-01127-3

Since it is not feasible to test every possible case before deployment, any AI system that is deployed in the real world must be monitored to ensure that it continues to deliver its advertised performance. This is especially necessary in high-stakes settings like national security and defense as well as decisions that affect an individual's employment, healthcare, housing, finances, etc. AI system users, including the government, industry, the public, and even AI experts, do not have the ability or resources to evaluate every output they receive. When deployers take responsibility to monitor system performance, trust in the AI system will increase.

To improve the economic competitiveness of U.S. AI systems, the AI Action Plan should:

1. **Create community standards for AI deployment and maintenance** that establish reasonable and responsible requirements to ensure AI systems maintain their advertised performance and behavior. The standards should (1) leverage the NIST AI Risk Management Framework[10] and related documents and (2) be developed with input from academia, industry, non-profits, and government deployers and users of AI systems.
2. Advocate **periodic assessment of AI system performance in each deployment, using newly collected data**. This assessment effort pays off in increased trust, by providing evidence that the AI system continues to perform as originally advertised. It also increases robustness, by providing an opportunity to detect and correct errors in a timely fashion.
3. Establish and maintain a confidential, voluntary **National AI Safety Reporting System.** This system could be modeled after the Aviation Safety Reporting System (ASRS), which collects confidential, voluntary reports about events, errors, and situations that lead to aviation safety concerns.[11] ASRS reports are aggregated and analyzed to identify ways to continually improve the National Aviation System. Similarly, the AI Action Plan should include a periodic analysis of AI safety reports to share lessons learned with industry, academia, government agencies, and the public.

Including AI literacy and AI system performance monitoring in the federal AI Action Plan will benefit the entire country by (1) empowering the general public to use AI products and services safely and effectively and (2) increasing trust and robustness for our deployed AI systems.

---

[10] Department of Commerce, Artificial Intelligence Risk Management Framework, NIST AI 100-1 (2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

[11] NASA Aviation Safety Reporting System, https://asrs.arc.nasa.gov/overview/summary.html