Response to Request for Information on the Development of an Artificial Intelligence (AI) Action Plan

To: National Science Foundation, U.S. Federal Register
From: IASA AI Architectures Community
Date: March 15th, 2025

1. Introduction: A Strategic Imperative for AI Leadership

Artificial Intelligence (AI) is redefining global competitiveness, economic growth, and national security. The United States must establish a proactive, innovation-driven AI policy that balances rapid technological advancement with ethical considerations, sustainability, and security. This response outlines strategic recommendations to guide the U.S. in maintaining its AI leadership. The modalities that need to be addressed are consumers of AI systems, and producers of AI applications. Consumers need safeguards and data privacy protections, while producers need to be consistent in their ability to innovate while staying within laws and regulations.

2. Building a Strong Foundation for AI Innovation

2.1. Investment in AI Research & Development (R&D)

- Increase federal funding for sovereign AI models, energy-efficient AI hardware, and AI-driven infrastructure.
- Establish public-private AI research labs to ensure continuous innovation.
- Incentivize U.S.-based semiconductor manufacturing to secure AI supply chains.
- Expand AI workforce development initiatives, including upskilling programs and AI literacy campaigns.

2.2. Supporting AI Adoption for Businesses

- Provide tax credits and funding grants for AI integration in small and medium enterprises (SMEs).
- Develop AI education and training programs to prepare workers for AI-driven industries.
- Establish an AI-Industry Council to guide policy across key sectors such as healthcare, finance, and defense.

3. Ensuring Ethical and Responsible AI

3.1. AI Transparency and Explainability

- Prioritize explainability in AI models, particularly in high-stakes applications such as healthcare and criminal justice.
- Mandate AI transparency laws requiring disclosure of AI decision-making processes.
- Encourage the development of self-regulating AI frameworks within industries.
- Consumers need to be able to easily access information from AI systems on how their data will be used, what data protections exist, and provide informed consent.
- End users should be warned that in probabilistic systems that hallucinations and confabulations are features of AI applications rather than bugs, and should use the outputs appropriately. This is one of the hardest goals to achieve in an operational AI environment, and guidance and a collaborative dissemination of what works would be helpful to drive positive outcomes.

3.2. Addressing Bias and Fairness

- Establish clear guidelines to mitigate bias and ensure fairness in AI applications.
- Promote the use of wide ranging training datasets to improve AI model scope and accuracy.

3.3. Strengthening AI Security

- Implement cybersecurity measures to protect AI systems from adversarial attacks and data breaches.
- Develop AI-driven cybersecurity solutions to safeguard critical infrastructure, such as the NIST AI RMF (Risk Management Framework).

4. Addressing AI’s Energy and Sustainability Challenges

4.1. Energy-Efficient AI Development

- Invest in energy-efficient AI models that minimize computational demands without sacrificing performance.
- Encourage liquid cooling and optimized AI chip technology to reduce energy consumption.

4.2. Renewable Energy for AI Infrastructure

- Expand federal incentives for renewable energy adoption in AI data centers that create American jobs.
- Support AI-driven grid modernization and energy storage solutions to balance electricity demand.

4.3. Research into Sustainable AI Technologies

- Promote research into sustainable AI innovations that align with national security interests.
- Encourage corporate commitments to sustainable AI operations with models, technology, and manufactured parts of American origin.

5. Preparing the Workforce for an AI-Driven Future

5.1. AI Education and Workforce Transition

- Expand AI training programs to equip workers with relevant skills for AI-driven industries, similar to typing and computer literacy programs in public K-12 schools.
- Promote AI literacy at all education levels to foster a broad understanding of AI technologies.
- Support workforce transitions in industries disrupted by AI through retraining initiatives.
- The creation of federally recognized AI professional certifications, as is seen in other professions (e.g. medicine, civil engineering), that can verify the AI systems meet the necessary requirements and standards to deploy to the general population. These certifications would be for both AI engineers as well as AI architects.

5.2. Public Awareness on AI Risks

- Develop self-learning resources and public education campaigns on AI-related cybersecurity risks.
- Establish programs and laws to counter AI-driven misinformation and deepfake threats.

6. Strengthening National Security and Global AI Collaboration

6.1. AI in Defense and Security

- Balance regulation with the ability to innovate for AI applications.
- Implement guidance on responsible AI use in defense applications to ensure compliance with national security standards.

6.2. AI Export Controls and Global AI Governance

- Foster international collaboration on AI research and governance frameworks that align with national security priorities.
- Promote the U.S. being at the center of AI innovation.

7. Driving Innovation, Competition, and Equitable AI Development

7.1. Supporting Startups and SMEs

- Provide funding and resources to foster AI innovation in startups and smaller enterprises.
- Streamline government procurement processes to encourage AI-driven solutions.

7.2. Ensuring Equitable AI Access

- Promote access to AI tools and resources across industries and regions.
- Encourage open-source AI development to enhance global AI collaboration.
- This collaboration must be done within the legal boundaries of what data can and cannot be shared across countries/municipalities.

8. Balancing Risk and Innovation with AI Governance

8.1. Defining AI Risk

- Use common sense risk tiering to understand the use case if the AI application falls.

8.2. Effective AI Governance

- Federal agencies need to clearly articulate the policies that govern their AI use cases, which can be adopted in the private sector.
- Organizations such as NIST should champion AI adoption frameworks that promote growth and safe adoption, and provide clear recommendations on how organizations of all sizes can ensure AI governance happens early with interdisciplinary SMEs (e.g. legal, compliance, finance) and continuously.

8.3. AI Best Practices

- Require continuous monitoring of AI outputs to ensure fidelity to the intended use cases, preventing AI systems from returning harmful outputs to consumers, and iterating upon future versions of AI applications using the monitoring results.

9. Conclusion: A Roadmap for AI Leadership

To maintain U.S. leadership in AI, we must:

- **Invest aggressively in AI R&D**
- **Ensure AI is developed responsibly and with sufficient economic incentives**
- **Address AI's sustainability challenges proactively**
- **Prepare the workforce for an AI-driven economy**
- **Enhance national security while the U.S. as the leader in AI R&D**

By implementing these strategic recommendations, the U.S. can continue to lead in AI innovation while safeguarding ethical, economic, and security interests. We look forward to further collaboration in shaping the AI Action Plan.

Sincerely,
IASA AI Architecture Community

This document is approved for public dissemination. The document contains no business-proprietary or confidential information. Document contents may be reused by the government in developing the AI Action Plan and associated documents without attribution.