

PUBLIC SUBMISSION

Received: May 28, 2025 Tracking No. nb8-ezvf-ab9n Comments Due: May 28, 2025 Submission Type: Web
--

Docket: NSF-2025-OGC-0001
NITRD_FRDOC_0001

Comment On: NSF-2025-OGC-0001-0001
Request for Information: Development of a 2025 National Artificial Intelligence Research and Development Strategic Plan

Document: NSF-2025-OGC-0001-DRAFT-0155
Comment on FR Doc # 2025-07332

Submitter Information

Organization: The Ohio State University

General Comment

This response to the NITRD NCO RFI regarding the 2025 update to the National Artificial Intelligence Research and Development Strategic Plan is submitted on behalf of The Ohio State University.

Attachments

Attachment1_The Ohio State University_RFI Response

A. What are the research needs and development challenges in AI that the Federal government should prioritize over the next 3 to 5 years?

AI Research Needs and Development Challenges: Federal Priorities (2025–2030)

As artificial intelligence continues to transform nearly every sector of society, the U.S. Federal government plays a critical role in steering research, infrastructure, and policy to ensure AI advances in ways that are innovative, secure, and competitive. We highlight below five key areas the government should prioritize:

1. National-Scale AI Computing Infrastructure

Challenge: State-of-the-art AI models, especially generative AI systems such as large language models (LLMs), Large Foundational Models (LFMs) and diffusion-based image generators, require enormous computational resources to train and evaluate. Academic and non-profit researchers are increasingly locked out of meaningful participation due to the prohibitive cost of compute and centralization of hardware in a few large corporations.

Federal Priority: Grow the National AI Research Resource (NAIRR) — a publicly funded, scalable AI computing infrastructure that is large enough to support:

- Training and fine-tuning of large models
- Access to GPUs/TPUs and high-bandwidth interconnects
- Open datasets and model repositories with usage incentives
- Secure environments for experimenting with sensitive or safety-critical AI
- Access to sandboxes, catering to both expert and novice users

Impact: This democratizes access to compute for academia, startups, and non-profit research labs, enabling innovation beyond industry gatekeepers and accelerating safe and trustworthy AI development.

2. Sustained Funding for Foundational AI Research

Challenge: While applied AI is rapidly advancing, many foundational questions in machine learning and AI remain unresolved, including issues related to generalization, interpretability, causality, robustness, and theoretical guarantees. New models and architectures are needed to make quantum advances in training and deployment of these models. Moreover, the emergence of these large-scale models and their practical goals towards science, engineering, and businesses will require innovations in all stages of computer architecture in the computing continuum, and networking systems from design to control and management. The emphasis on short-term, application-focused results often sidelines deeper, longer-horizon research critical to accelerate these advances.

Federal Priority: Significantly expand support for long-term use-inspired foundational research, including:

Theory of learning, optimization, and generalization

- Representation learning and disentangled features
- Multi-agent systems and emergent behavior
- Causality, fairness, and explainability

- Safe and aligned reinforcement learning
- Formal verification and provable guarantees

New generation systems architectures that support

- Instruction sets, data representation, execution units
- Networking technologies (energy-aware data movement protocols, topologies, collective algorithms)
- Edge devices (support for energy-aware computation, I/O, and communications)
- Programming models (efficient support for point-to-point and collective communication across the computing continuum)
- Memory technologies (disaggregated memory)
- High-performance I/O (storage technologies and file systems, I/O protocols).

Research support should come not only from NSF and DARPA but also mission-driven agencies (NIH, DOE, DoD) that provide the use-inspired context to propel fundamental advances. In this way, the government can ensure a diversified and interdisciplinary research agenda to meet its needs.

Impact: Such investment ensures that U.S. researchers remain leaders in core algorithmic innovation and builds a foundation for next-generation AI systems that are trustworthy, robust, and aligned with human values.

3. Research on Edge AI to Democratize AI Deployment

Challenge: Most AI systems today require cloud-based infrastructure, limiting their utility in resource-constrained, privacy-sensitive, or connectivity-limited environments (e.g., rural health care, disaster zones, home robotics). Reliance on centralized cloud-based AI creates disparities in access and introduces serious concerns around surveillance, data privacy, and latency.

Federal Priority: Fund targeted research and development in Edge AI, including:

- Lightweight, energy-efficient model architectures
- Federated and decentralized learning algorithms
- On-device AI for smartphones, wearables, and embedded systems
- Secure model update and inference pipelines
- Standardization of edge AI toolchains and benchmarking

Additionally, support targeted testbeds and pilot programs across critical domains (e.g., agriculture, public safety, education, smart infrastructure) that showcase the value of edge AI in varied environments.

Impact: Edge AI can expand the reach of AI to new markets and sectors while enhancing privacy and fostering system security and resilience by reducing reliance on centralized systems.

4. Responsible AI: Reliability, Robustness, and Alignment

Challenge: As AI systems grow more capable and autonomous, ensuring that they behave as intended—reliably, repeatably, and safely—becomes a central technical challenge. Failures of generalization, susceptibility to adversarial inputs, distributional shifts, and

misalignment with user intent are increasingly common and high-risk. Investments in these areas will ensure the U.S. maintains strategic leadership in secure and responsible AI. This is especially important where market interest lags national interest.

Federal Priority: Invest in the science of reliable AI systems, focusing on:

- Secure-by-design AI architectures resilient to adversarial threats
- Robustness to noise, domain shift, and adversarial manipulation
- Continual and adaptive learning without catastrophic forgetting
- Mechanisms for detecting and mitigating failures or hallucinations
- Formal verification, interpretability, and runtime monitoring
- Methods to detect and mitigate misuse of foundation models (e.g., for cyber offense)
- Verifiable AI agents for critical applications like firmware analysis, reverse engineering, and cyberspace defense
- Co-design of AI safety and security in autonomous systems to prevent both unintentional failures and deliberate attacks

Impact: This expands the scope of responsible AI into engineering rigor—ensuring AI systems are dependable, auditable, and safe to deploy in mission-critical applications such as healthcare, finance, and national security.

5. Employment and Workforce Development

Challenge: Institutions of higher learning, including community colleges, will continue to serve as critical drivers of innovation and developing the AI-enabled workforce of the future. What kinds of skills are needed by these workers to work most effectively with new technologies? How can they be prepared through retraining or moving to other positions to continue to be productive in the face of AI? Traditional degrees and credentialing alone will prove insufficient to produce AI talent at scale.

Federal Priority: Education and training should prioritize the development and enhancement of core AI competencies that enhance enterprise productivity.

- Support for research to understand the impact of AI on workers and businesses and the skill sets required for workers at all levels of education to work in the new AI economy.
- Federal and state governments should leverage incentives to facilitate employee training at institutions where they can learn to utilize AI to drive innovation.
- Universities can adopt the extension-centers model, analogous to that of agricultural colleges, to deliver education and training.
- Invest in education pipelines that integrate AI and cybersecurity, funding curriculum development, REUs, and fellowships to grow a workforce capable of developing AI systems that are not only powerful but also safe, secure, and aligned with national priorities.

Impact: Successful deployment and adoption of AI necessitate a highly skilled AI workforce and AI-knowledgeable domain experts. Federal support for workforce development will ensure that the U.S. remains a leader in AI implementation and deployment across industries.

B. What are ideas for novel mechanisms for research partnerships (of the Federal government) with industry and/or academia?

To accelerate secure and responsible AI innovation, the Federal government should establish mission-driven, long-term research partnerships that unite academia, industry, and national laboratories around high-impact, non-commercial challenges in AI outlined above. This includes

- Creating AI security consortia focused on adversarial robustness and misuse mitigation
- Building shared AI cyber ranges where researchers can safely evaluate model behavior under adversarial conditions
- Incentivize industry foundation partnerships with academic institutions to create “AI Universities”
- Continue to expand the NSF-funded AI Institutes ecosystem supporting use-inspired, fundamental breakthroughs via a funding model built around co-funding across federal agencies

C. Conclusion

To ensure U.S. leadership in AI while promoting rapid innovation and societal benefit, the Federal government must strategically invest in:

- Shared infrastructure to level the playing field,
- Foundational research that advances theory and long-term capabilities,
- Edge AI to make AI truly ubiquitous
- Responsible AI, and
- Education and Workforce Development to effectively train an AI-ready workforce.

These efforts must be coordinated across agencies, supported by open-access initiatives, and complemented by robust workforce development, ethical oversight, and public-private collaboration.

“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 2025 National AI R&D Strategic Plan and associated documents without attribution.”