PUBLIC SUBMISSION

Received: May 07, 2025
Tracking No. mae-ez1z-2osl
Comments Due: May 28, 2025 **Submission Type:** API

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-0063
Comment on FR Doc # 2025-07332

Submitter Information

Organization: Cyber Institute

General Comment

Please see attached file.

Attachments

NSF RFC RESPONSE

CYBER INSTITUTE

5 UNION SQUARE WEST, SUITE 1124, NEW YORK, NY 10003 • 800.357.8315 • WWW.CYBER-INSTITUTE.ORG

Learning Globally • Serving Locally

May 7, 2025

National Science Foundation
Networking and Information Technology Research and Development
National Coordination Office
2415 Eisenhower Avenue
Alexandria, VA 22314

Re: Request for Information on the Development of a 2025 National Artificial Intelligence (AI) Research and Development (R&D) Strategic Plan

Dear National Science Foundation:

On behalf of the Cyber Institute, we respectfully submit the following response to the Request for Information (RFI) regarding the development of the 2025 National Artificial Intelligence (AI) Research and Development (R&D) Strategic Plan (Docket ID No. NSF-2025-OGC-0001). We commend the National Science Foundation and the National AI Initiative Office for taking a comprehensive, thoughtful, and forward-looking approach to guiding the future of AI research and development in the United States.

We are particularly encouraged by the emphasis on prioritizing R&D in areas less likely to attract private-sector funding. We recognize the federal government's critical role in areas vital to national security, scientific discovery, infrastructure resilience, and ethical governance. The focus on high-risk, high-reward foundational research aligns with the historic successes of government-funded initiatives in AI, such as the development of neural networks and reinforcement learning. Further, the commitment to aligning the 2025 National AI R&D Strategy with the AI Action Plan reflects a sophisticated understanding of the interconnected nature of AI development, regulation, and public interest objectives.

Topics Addressed in This Comment

- Governance
- Research Integrity
- Public-Private Collaboration
- National Security
- Reproducibility and Standards
- Ethical AI Development

The Cyber Institute fully supports these strategic directions and offers detailed comments to help advance these aims.

1. National AI Risk Maturity Model (ARMM)
The current strategy appropriately highlights the need to prioritize AI research that addresses national interests over immediate commercial gains. However, there is a gap in systematic frameworks to assess research risks and opportunities across domains. The Cyber Institute's study, Artificial Intelligence in Cybersecurity: A Survey of National Research, Investment and Policy Implementation (2023), demonstrates that structured maturity models enable better risk anticipation and resource allocation. An AI Risk Maturity Model (ARMM) would categorize projects by dual-use potential, societal impact, generalizability, and adversarial vulnerability. ARMM would allow NSF to prioritize funding based on technical merit and national strategic value.

Recommendation: *Develop and implement an AI Risk Maturity Model (ARMM) to guide strategic funding decisions and oversight across AI research initiatives.*

2. Technical Foundations for Robust and Traceable AI Systems.
We applaud the emphasis on AI system security and reliability. However, critical technical areas such as model lineage tracking, dataset auditability, and AI forensic tools remain underexplored in the private sector due to weak immediate market incentives. As detailed in the Cyber Institute's Examination of Applications of Artificial Intelligence in Cybersecurity: Strengthening National Defense with AI (2023), data and model integrity vulnerabilities have direct national security implications. Investment in foundational methods like watermarking and secure training data provenance tracking is crucial for building trustworthy AI ecosystems that support infrastructure, defense, and economic stability.

Recommendation: *Expand federal investments in AI security technologies, including model lineage, dataset audibility, watermarking, and AI forensic capabilities.*

3. Good AI Research Practices (GARP)
The emphasis on reproducibility and open science is highly commendable. Nevertheless, reproducibility efforts may remain inconsistent across research domains without standardized procedures. Drawing from insights in Quantum Computing Policy and Strategy Recommendations (Cyber Institute, 2022), standardized frameworks were critical in adjacent emerging technology fields. A "Good AI Research Practices (GARP)" initiative would create a common baseline for secure, transparent, reproducible AI research outputs, including mandatory training data disclosures, model documentation, and reproducibility benchmarks for federally funded projects.

Recommendation: *Establish "Good AI Research Practices (GARP)" to ensure consistency, security, and transparency in federally funded AI research.*

4. Addressing Dual-Use Risks and Misuse Prevention.
The current plan wisely acknowledges the importance of addressing national security concerns associated with AI advancements. However, more targeted research is needed into dual-use risks, adversarial robustness, and AI misuse prevention. The Cyber Institute's Geopolitical Implications of Artificial Intelligence in Cybersecurity (2023) highlights how adversaries increasingly exploit emerging technologies for strategic advantage. Proactive research into threat modeling, red-teaming practices, and mitigation strategies will bolster U.S. preparedness and resilience.

Recommendation: *Fund dedicated programs in AI red-teaming, dual-use threat modeling, and proactive misuse prevention research.*

5. Ethical Governance Research and Public-Interest AI Consortia.
We strongly support the focus on broad societal benefits in AI development. However, ethical governance research often lacks private sector funding due to limited market incentives, as shown in "The Hidden Costs of AI Ethics" (Raji et al., 2020) and "Ethics as a Service" (Morley et al., 2021). Critical ethical, safety, and governance frameworks may not be adequately developed without government intervention. We recommend the creation of "AI Governance Labs", multidisciplinary, federally funded consortia tasked with experimental research on responsible innovation, real-world governance testing, and practical standards development. By prioritizing ethical governance, the United States will maintain global leadership in technological excellence and in setting values-based standards for AI deployment.

Recommendation: *Establish federally funded "AI Governance Labs" to develop ethical, safe, and globally trusted AI systems.*

These comments are submitted on behalf of Cyber Institute in response to the National Science Foundation's Request for Comments on Docket ID No. NSF-2025-OGC-0001.

Point of Contact
Dr. Taylor Rodriguez Vance
Cyber Institute