PUBLIC SUBMISSION

Received: May 02, 2025
Tracking No. ma6-u2hq-xlnb
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-0036
Comment on FR Doc # 2025-07332

Submitter Information

Name: Mitchell Berger

General Comment

Dear Mr. D'Souza: I write to encourage the Networking and Information Technology Research and Development (NITRD) Program and others to consider the topics of dual use considerations and consent, privacy and confidentiality as key priorities in revising the National Artificial Intelligence Research and Development Strategic Plan (2023 Update) and developing future priorities. Full comment is below. Sincerely, Mitchell Berger

Attachments

airesearchplan522025mb

From: Mitchell Berger, (comments made in personal capacity)

Re: Request for Information on the Development of a 2025 National Artificial Intelligence (AI) Research and Development (R&D) Strategic Plan, https://www.federalregister.gov /documents/2025/04/29/2025-07332/request-for-information-on-the-development-of-a-2025-national-artificial-intelligence-ai-research [Docket NSF-2025-OGC-0001]

Date: May 2, 2025

Dear Mr. D'Souza: I write to encourage the Networking and Information Technology Research and Development (NITRD) Program and others to consider the topics of dual use considerations and consent, privacy and confidentiality as key priorities in revising the National Artificial Intelligence Research and Development Strategic Plan (2023 Update) and developing future priorities.

Citing a recent Executive Order (EO),[1] the Federal Register announcement asks for input about how the National AI R&D Strategic Plan 2023 Update can be revised to reflect current Administration priorities, including the forthcoming Artificial Intelligence Action Plan.[2]

The revised Strategic Plan should consider Dual Uses as a priority: The National Artificial Intelligence Advisory Committee: Year-Two Insights Report (May 2024)[3] and FINDINGS: The Potential Future Risks of AI report (Oct. 2023) [4] do note the importance of addressing potential AI misuse. But neither these reports nor the recent 2023 Strategic Plan update address the issue of dual use AI technologies. As one author explains, citing a recent example of ChatGPT misuse:[5] "[w]hile AI enhances healthcare, education, and logistics, the same technology can be used to execute fraudulent activities, cyberattacks, and misinformation campaigns." The U.S. AI Safety Institute (US AISI) at the National Institute of Standards and Technology has considered some of these issues, as in its recent draft Updated Guidelines for Managing Misuse Risk for Dual-Use Foundation Models.[6] NIST and its partners also issued guidance for software developers[7] and an AI Risk Management Framework for generative AI that considers these issues.[8] The likelihood that AI models developed for public and expert use, which have many

[1] EO 14179, https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence
[2] https://www.nitrd.gov/national-artificial-intelligence-research-and-development-strategic-plan-2023-update/; https://www.whitehouse.gov/briefings-statements/2025/02/public-comment-invited-on-artificial-intelligence-action-plan/
[3] https://ai.gov/wp-content/uploads/2024/06/National-Artificial-Intelligence-Advisory-Committee_Year-Two-Insights-Report.pdf
[4] https://ai.gov/wp-content/uploads/2023/11/Findings_The-Potential-Future-Risks-of-AI.pdf
[5] https://www.orfonline.org/expert-speak/the-rising-threat-of-dual-use-technology-a-looming-crisis-in-the-age-of-ai
[6] Updated Guidelines for Managing Misuse Risk for Dual-Use Foundation Models, https://www.nist.gov/news-events/news/2025/01/updated-guidelines-managing-misuse-risk-dual-use-foundation-models
[7] Booth H, et al. (2024) Secure Development Practices for Generative AI and Dual-Use Foundation AI Models: An SSDF Community Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-218A. https://doi.org/10.6028/NIST.SP.800-218A
[8] https://www.nist.gov/itl/ai-risk-management-framework

potential benefits, could be intentionally or even unintentionally or carelessly misused to cause harm should be explored in the revised Strategic Plan and be identified as a priority for further research.[9] Research and programs on this issue potentially fall within several areas of the 2023 Strategic Plan including especially Strategies 2 (Human-AI Interactions); 3 (Ethics) and 4 (Safety). Key partners in addition to NITRD could include NIH, which could help place AI in the context of other dual use research,[10] the Cybersecurity and Infrastructure Security Agency and Office of Science and Technology Policy.

The revised Strategic Plan should emphasize consent to share information as part of privacy and confidentiality considerations: Recent reports from the NAIAC such as those concerning Data Challenges and Privacy Protections for Safeguarding Civil Rights in Government,[11] and the Potential Future Risks of AI Findings report developed in 2023 do discuss privacy but fail to emphasize the importance of individuals consenting as to how their information is shared and used, how consent will be operationalized, whether once given by an individual or entity it can be subsequently withdrawn, how individuals and entities will be informed of any unauthorized breaches in which information is obtained and similar issues.[12] The 2023 Strategic Plan also discusses privacy in several areas but does not consider such issues as consent, federal, state, territorial, local and tribal statutes and regulations and international considerations.[13] Concerning recent examples such as use of individuals' images in facial recognition systems, for health care data mining and at the retail sales level underscore the need for further research and a strong privacy, confidentiality and ethics framework and research agenda.[14] This is consistent with the current 2023 Strategic Plan Update's Sections 2 (Human-AI interaction) and 3 (Ethics) but in some ways should be part of each of the six main strategies. For instance, standards and benchmarks and performance measures (Strategy 7) and international collaboration can help build consensus on these issues.

Thank you for your consideration of this input.

Sincerely,

Mitchell Berger Note/Disclosure: I am submitting these suggestions solely in my personal/private capacity. The views expressed are mine only and should not be imputed either to other individuals or to any public or private entity.

[9] See e.g., https://councilonstrategicrisks.org/2024/07/12/advances-in-ai-and-increased-biological-risks/;https://www.governance.ai/analysis/managing-risks-from-ai-enabled-biological-tools; https://www.ai-frontiers.org/articles/ais-are-disseminating-expert-level-virology-skills

[10] https://grants.nih.gov/grants/guide/notice-files/NOT-OD-25-061.html#:~:text=The%20DURC/PEPP%20Policy%20addresses,of%20scientific%20and%20technological%20risks.

[11] https://ai.gov/wp-content/uploads/2024/06/RECOMMENDATION_Data-Challenges-and-Privacy-Protections-for-Safeguarding-Civil-Rights-in-Government.pdf

[12] https://ai.gov/wp-content/uploads/2023/11/Findings_The-Potential-Future-Risks-of-AI.pdf

[13] https://ovic.vic.gov.au/privacy/resources-for-organisations/artificial-intelligence-and-privacy-issues-and-challenges/; https://www.ibm.com/think/insights/ai-privacy

[14] https://www.jdsupra.com/legalnews/artificial-intelligence-demands-8410801/; https://www.enzuzo.com/blog/ai-privacy-violations; https://www.linkedin.com/pulse/real-world-examples-ai-data-privacy-breaches-jean-ng--kkcac