WORLD **PRIVACY** FORUM

Comments of World Privacy Forum
To Networking and Information Technology Research and Development (NITRD)
National Coordination Office (NCO), National Science Foundation
Regarding Request for Information on the Development of an Artificial
Intelligence (AI) Action Plan

Sent via email to ostp-ai-rfi@nitrd.gov

AI Action Plan
Attn: Faisal D'Souza, NITRD NCO
2415 Eisenhower Avenue
Alexandria VA 22314
USA

14 March 2025

The World Privacy Forum appreciates the opportunity to respond to the Request for Information on the Development of an Artificial Intelligence (AI) Action Plan. The RFI is requested by the NITRD NCO, National Science Foundation, on behalf of the Office of Science and Technology Policy (OSTP) and was published February 6, 2025 at 90 FR 9088, https://www.federalregister.gov/documents/2025/02/06/2025-02305/request-for-information-on-the-development-of-an-artificial-intelligence-ai-action-plan .

The World Privacy Forum (WPF) is a respected non-profit public interest research group focused on conducting research and analysis regarding complex data ecosystems and their governance and privacy, with a focus on identity, AI, and health, among additional areas. WPF works extensively across multiple jurisdictions, including the U.S., India, Asia, Africa, the E.U., and additional jurisdictions. WPF is a non-profit member of the NIST AI Safety Institute Consortium, focusing on research. At the OECD, WPF's Executive Director serves on the Global Partnership on AI's (GPAI) Steering Committee and leads the AI work for civil society at the AI Working Party at OECD. WPF participated in the first (2018) core group of AI experts that worked on the OECD Recommendation on Artificial Intelligence, now widely viewed as normative principles for AI. Recently, WPF participated in the 2024 update to the AI

Recommendation. In other work, WPF co-chairs the UN Statistics Data Governance and Legal Frameworks working group, and serves as a special advisor to the WHO's HDC board. WPF has presented its research on complex data ecosystems governance and privacy to the National Academies of Science, the Mongolian Academies of Science, and the Royal Academies of Science. Recent WPF research publications and datasets include *The Global Table of Privacy Laws, Conventions, and Treaties*, the most comprehensive research in this area and the first to be conducted to the ISO M49 Standard. Another recent publication is *Risky Analysis*, a report indexing and analyzing global AI Governance tools and AI implementation. In February this year, WPF held a half-day tutorial at the IEEE WACV Conference where computer vision scientists presented new papers on advanced topics connected to AI governance and privacy in the area of health. See the World Privacy Forum website for more information about our work, https:// www.worldprivacyforum.org.

In response to the RFI, WPF recommends prioritizing the following items:

I. Prioritize support for NIST's AISIC and participate in the growing global network of AISIs

The NIST AI Safety Institute Consortium (AISIC) is among a growing network of national AISIs, or AI Safety Institutes. In November 2024, technical AI experts from the U.S., the E.U., the UK and seven additional countries' AISIs met in San Francisco for the inaugural meeting of the AISI International Network. The AISIs are a recent and important multi-governmental structure that -- while embryonic now -- will likely grow and hold a place of increasing significance in the coming years.

We are concerned that the U.S. government's support of the U.S. AISIC may have diminished, and concomitant with this, potentially also U.S. leadership among the global AISIs. For example, in February 2025 at the influential Paris AI Action Summit and week, which WPF attended, the U.S. AISIC was notably absent from dialogues and panels where other AISIs were prominently featured and their views discussed. While the NIST AISIC had an early start, the AISIs in other jurisdictions are now beginning to catch up to and potentially move past the U.S. efforts in terms of their staffing, expansion of research tasks, and overarching influence in the AI global network. Fully funding, staffing, and robustly supporting NIST's AISIC efforts needs to be an integral and high priority aspect of the AI Action Plan.

II. Prioritize the advancement of AI governance tools by supporting AI governance tools research and development

AI governance tools form a pivotal component of the management of AI systems. WPF defines AI governance tools as:

> "Socio-technical tools for mapping, measuring, or managing AI systems and their risks in a manner that operationalizes or implements trustworthy AI." (*Risky Analysis*, WPF, December 2023).

AI governance tools are increasingly common and are poised to become an integral part of the evolution of AI analytical architecture. It is reasonable to make the assessment that AI governance tools that can automate and scale the assessment of the accuracy, reliability, fitness, and overall trustworthiness of AI systems will become part and parcel of how AI systems are managed. However, there are many challenges in the area of AI governance tools, the first of which is that many more AI governance tools are needed, and high quality tools will need to be researched and built. The best possible AI governance tools will be properly fit to the AI system in question, built to standards, and will effectively address the AI system problems or issues they are intended to address. There is a dearth of such tools right now, and this can be remedied if creating such tools is made a priority. There is also a dearth of quality control mechanisms for AI governance tools, which is discussed in item III, below.

The importance of effective, high-functioning, and trustworthy AI governance tools cannot be overstated. Anyone seriously working with AI ecosystems and AI governance understands, deeply so, that AI governance will be automated, at scale, and that AI tools will be among the needed items to accomplish this. It is too easy to miss the importance and criticality of tools that sit at the implementation layer of AI systems, which is why we encourage OSTP to ensure AI governance tools and their metrology are made a priority in the AI Action Plan.

III. Prioritize advancing the trustworthy metrology of AI governance tools by supporting the building of an evaluative environment and evidentiary foundation with which AI governance tools themselves can be tested, improved, and validated

The second major challenge with AI governance tools is that the gap in the metrology of AI governance tools creates an environment where AI governance tools can be used, but not always fully trusted. This is occurring because the tools that do exist generally lack an evaluative environment in which the effectiveness of the tools can be measured. AI governance tools are nascent, and are often not subject to evidence-based assessments or quality assurance mechanisms, or for that matter, standards.

AI governance tools are necessary to measure how AI systems are functioning, and offer the promise of improving the understanding of various aspects of AI systems and their implementations. However, AI governance tools must themselves also be effectively measured for accuracy and trustworthiness. This is a major gap area in AI governance. We encourage OSTP to give high priority to support the creation of systematic guidance, testing, procedures, and oversight mechanisms to ensure that the context, use, and interpretation of AI governance tools is trustworthy. WPF has written extensively about this issue, with case studies, a global index of AI governance

tools governments are using, and suggested standardization models for AI governance tools. *Risky Analysis, Assessing and Improving AI Governance Tools*, https://www.worldprivacyforum.org/2023/12/new-report-risky-analysis-assessing-and-improving-ai-governance-tools/ (ePub also available.)

IV. Prioritize and support the use of Voluntary Consensus Standards for AI-enabled medical devices and support study of AI governance tools that monitor AI-enabled medical devices

For more than 20 years the FDA has utilized Voluntary Consensus Standards (VCS), conducted under OMB A-119 rules, to develop a bespoke standard for each FDA-approved medical device. The VCS standards are publicly available in a database, https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm . In its guidance, the FDA has recommended that VCS are also used in the current roster of more than 1,000 AI-enabled medical devices. WPF urges OSTP to support this position so as to encourage the creation of A-119 VCS standards for each AI-enabled medical device. WPF believes this will go far to creating higher quality AI-enabled medical devices.

WPF also urges OSTP to prioritize the study of how AI governance tools interact with AI-enabled medical devices. AI-enabled medical devices often utilize AI governance tools in order to detect levels of noise or algorithmic fit issues that would cause reduced effectiveness of medical devices or cause medical device malfunction. AI governance tools used to detect quality control in medical devices must themselves be fit for purpose and tested for effectiveness.This is an issue well worth prioritizing.

V. Conclusion

Thank you for the opportunity to submit comments regarding prioritization in the AI Action Plan. Please let us know if you would like additional data or research on any of the topics we have discussed in the comments.

Respectfully submitted,

Pam Dixon,
Executive Director
World Privacy Forum

Per the request specified in 90 FR 9088, WPF affirms the following:

"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."