



88 Colin P Kelly Jr Street,  
San Francisco, CA 94107  
Tel: +4915563316291  
mlinks@github.com

October 24, 2025

Stacy Murphy  
Deputy Chief Operations Officer/Security Officer  
Office of Science and Technology Policy  
Executive Office of the President  
1650 Pennsylvania Ave., NW  
Washington, DC 20504

Subject: GitHub Response to “Request for Information; Regulatory Reform on Artificial Intelligence,” Docket ID OSTP-TECH-2025-0067

Dear Ms. Murphy:

GitHub appreciates the opportunity to provide input to the White House Office of Science and Technology Policy (OSTP) on regulatory reform for artificial intelligence (AI). As the world’s leading platform for software development, GitHub is home to a vibrant ecosystem of open source software and open source AI innovation, supporting over [23 million developers](#) in the United States and [150 million worldwide](#). GitHub is both a provider of the world’s leading AI powered software development tools and a host of the full stack of open source AI components. We are committed to advancing responsible and secure AI development, and to ensuring that regulatory frameworks foster innovation and sustain the open source developer community. In this submission, we identify opportunities for the U.S. federal government to provide additional clarity and guidance to reduce uncertainty and lower barriers to AI adoption and innovation.

## **Support Open Source and Open Weight AI Development**

AI policies should support open source and open weight model development and sharing, especially when the marginal risk is comparable to proprietary development or can be mitigated. This should be paired with clear obligations on use, distribution, and disclosure, consistent with the National Institute of Standards and Technology (NIST) [AI Risk Management Framework](#) (RMF). This approach encourages reproducibility, competition, and public interest research without imposing excessive and imbalanced compliance burden on open source community projects that rely on volunteer maintainers.

Open source licenses are foundational for GitHub-hosted projects, supporting developer autonomy, interoperability, and legal clarity. Many OSS projects on

GitHub rely on volunteer maintainers, and heavy compliance requirements or regulatory restrictions on downstream use—such as those proposed in some state-level AI bills—would fragment ecosystems, undermine collaboration, and make it impossible to release a model under an open source license. Instead of imposing such burdens, policymakers should prioritize standards-based disclosures and targeted misuse enforcement to sustain innovation and participation in the open source community.

## **Clarify Text and Data Mining (TDM) Exceptions and Support Open Data**

Federal agencies should clarify that text and data mining (TDM) for AI training and research is permissible under existing copyright law, as uncertainty around legal risk inhibits innovation, especially for researchers, startups, and open source developers. Clear guidance affirming TDM for research and development as permissible fair use can reduce barriers to entry and foster a more robust AI research and innovation ecosystem.

America's [AI Action Plan](#) called for leveraging the National AI Research Resource (NAIRR) Pilot and partnering with the private sector to increase the research community's access to computing, models, data, and software resources. GitHub encourages the federal government to build on this momentum by investing in and expanding open data initiatives to advance AI training and evaluation. This means increasing the availability of government datasets as open data, supporting the creation of open source tools for data access and processing, and incentivizing industry-led open data efforts. Open data is essential for reducing costly barriers to entry, democratizing AI research, and empowering researchers, startups, and open source developers to accelerate innovation. Making high-quality datasets openly accessible enhances reproducibility, drives breakthroughs, and creates new opportunities for smaller players to compete and innovate.

## **Promote Interoperable Standards**

Developers and platforms are struggling to keep up with fragmented and conflicting AI regulations across U.S. states and global jurisdictions. The federal government should act as a centralizing force by promoting interoperable and open source standards and tools to meet regulatory requirements, such as [C2PA](#) for content provenance, and providing clear implementation guidance, rather than mandating proprietary watermarking tools or closed systems. OSTP should also support NIST's work on AI dataset and model documentation and incentivize the adoption of standardized practices for developers. In developing standards and guidance for issues such as content provenance and documentation, agencies should avoid imposing enterprise-style reporting requirements on small open source projects; instead, agencies should encourage open standards and offer templates and tooling that can be integrated into developer workflows.

## **Establish Frontier AI Threshold**

Federal agencies can reduce uncertainty and regulatory fragmentation by establishing clear, uniform federal thresholds for what constitutes a "frontier" or

“large” AI model, replacing the current patchwork of state-level regulations that use varying criteria such as compute usage or annual revenue. The U.S. government should clarify that fine-tuning or adapting an existing large model does not confer frontier developer status and ensure that open source contributors are not unintentionally included in high-risk categories. A consistent federal standard will provide regulatory certainty, protect innovation, and focus oversight on areas of genuine systemic risk.

## Support AI and OSS Cybersecurity

As AI systems become increasingly essential to critical infrastructure and services, robust cybersecurity is essential to safeguard innovation and public trust. Federal policy should align AI-accelerated software development lifecycles with the NIST [Secure Software Development Framework \(SSDF\)](#) and the NIST AI RMF, encouraging secure-by-design practices throughout the AI stack. Procurement and compliance frameworks should be updated to recognize open source security tools as valid controls.

Open source security is a critical foundation for AI cybersecurity, as much of the AI ecosystem relies on open source components maintained by the global developer community. To strengthen the security of AI systems, it is vital to fund and sustain the open source dependencies that underpin them. The [GitHub Secure Open Source Fund](#) supports maintainers working on critical open source projects through providing funding directly linked to improving OSS security. The U.S. [Open Technology Fund](#)'s [Free and Open Source Software Sustainability Fund](#) could be used as a model for funding critical open source dependences, building resilience across the AI supply chain and the entire software ecosystem.

## Address Barriers to Government Use of AI Developer Tools

Current federal IT policies and some agency-level directives often impose blanket bans on generative AI tools, treating all use cases as inherently high-risk and limiting the government’s ability to benefit from modern AI developer technologies. The U.S. Government Accountability Office report on [Generative AI Use and Management at Federal Agencies](#) identified complying with federal policies and guidance and maintaining up-to-date appropriate use policies as barriers to using generative AI tools. To reduce these barriers, federal agencies could replace such prohibitions with risk-based allow-lists, in accordance with [OMB M-25-21](#). This approach would define specific, permitted uses—such as internal code suggestions operating behind enterprise controls—while requiring robust logging and traceability. Additionally, applying the NIST AI RMF in acquisition and Authorization to Operate (ATO) processes would ensure that AI tools are adopted responsibly, enabling agencies to benefit from AI-powered developer tools while maintaining appropriate oversight and security.

## Conclusion

GitHub appreciates the opportunity to contribute to OSTP’s RFI on regulatory reform for AI. By clarifying legal frameworks, promoting interoperable standards, and establishing clear thresholds for frontier AI, the federal government can

reduce uncertainty and compliance burden for developers while fostering innovation, security, and global leadership in AI. By supporting open data initiatives and critical open source dependencies, the U.S. can strengthen security and innovation at scale, setting a global standard for AI leadership.

Sincerely,

A handwritten signature in black ink, appearing to read "m1z".

Mike Linksvayer  
VP, Developer Policy  
GitHub  
[mlinksva@github.com](mailto:mlinksva@github.com)