NASEM Workshop | Washington DC | April 3, 2025

Responsible Development & Dissemination of AIxBio Models

Navigating the Benefits & Risks of Publishing Studies of In Silico Modeling and Computational Approaches of Biological Agents and Organisms

NTI
BUILDING A SAFER WORLD

NTI:bio

Overview

- Bio Funders Compact
- AIxBio Model Dissemination & Biosecurity
- Managed / Tiered Access
- Key Takeaways

Bio Funders Compact

Theory of Change

- Bio Funders Compact: A public commitment by funders of bioscience & biotech research to incorporate pre-funding biosecurity review into decision-making
- Reduce the probability that funders will support unduly risky bioscience research
- Provide strong incentives for scientists & technologists to adhere to biosecurity and biosafety best practices

- Three founding signatories

The international Bio Funders Compact launched at the Global Health Security Conference in June 2024

Bio Funders Compact Commitments

We, as funders of life science research, acknowledge the leverage we have to incentivize safer and more secure practices. We accept our role in safeguarding the tools of modern bioscience and biotechnology against accidental and deliberate misuse, and thus commit to:

1. Implement pre-funding biosecurity and biosafety reviews as part of the decision-making processes within our organization.
2. Conduct post-funding assessments of adherence to biosecurity and biosafety best practices among researchers that we fund.
3. Develop implementation plans to fulfill this pledge while focusing on the mission and needs of our respective organizations.
4. Designate an individual or team to oversee biosecurity and biosafety pre- and post-funding reviews as well as other activities that align with this pledge.
5. Share best practices for biosecurity and biosafety risk assessment and risk reduction among the bioscience and biotechnology funding communities.

AIxBio Model Dissemination & Managed Access

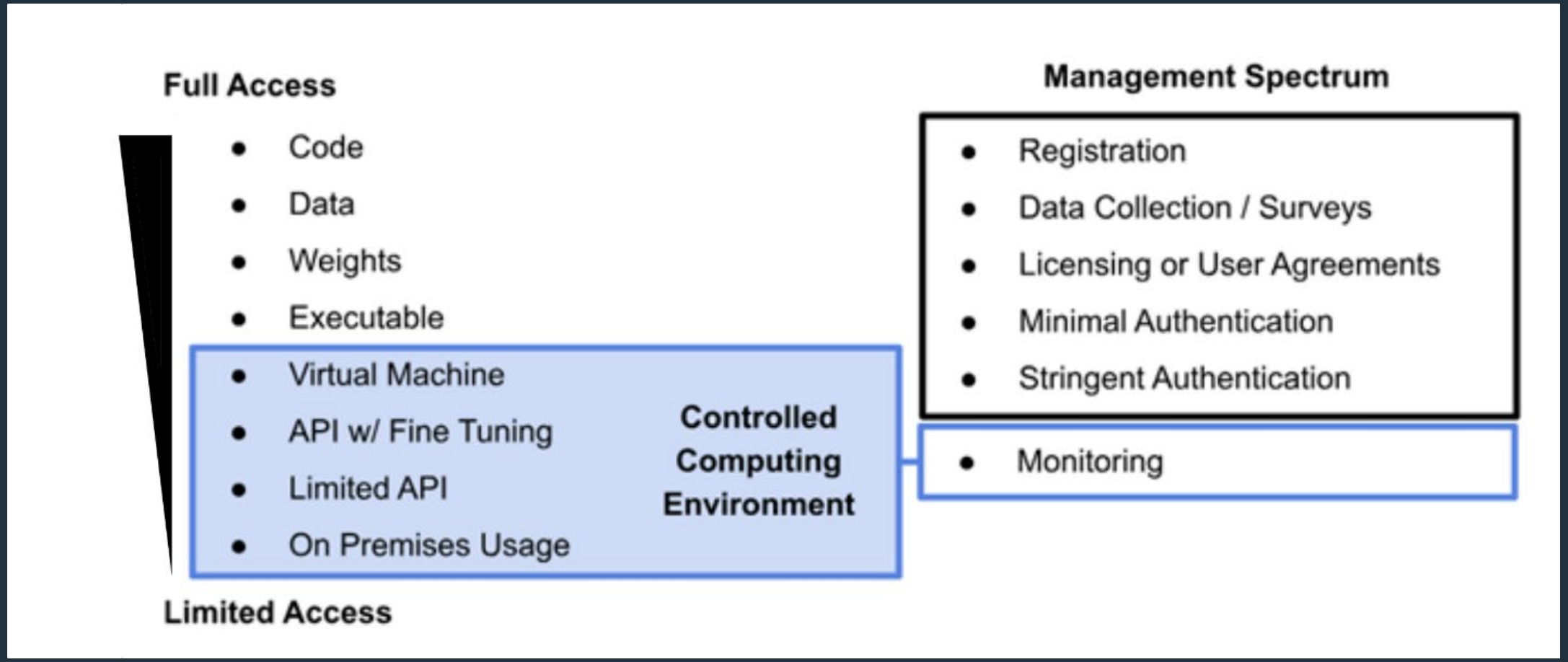
- AIxBio model dissemination is a key consideration for biosecurity
- Managed access can play an important role in safeguarding tools against misuse
- Could help build public trust in scientific communities

Managed Access Principles

- It is important & feasible to balance security with equitable access to tools – benefits depend on access
  - CEPI is establishing managed access frameworks which prioritize equitable access along with responsible dissemination & biosecurity
- Tiered frameworks will be essential
  - Some tools are low risk and will not need managed access
  - For tools with higher risk:
    - Users should meet some criteria for access
    - More access should require more stringent criteria

NTI 2024 Report on Guardrails for AI Biodesign Tools

Options for Managed Access



Managed Access International AI Safety Report

Level of Access	What It Means	Examples	Traditional Software Analogy
Fully Closed	Users cannot directly interact with the model at all	Flamingo (Google)	Trading algorithms used by private hedge funds
Hosted Access	Users can only interact through a specific application or interface	Midjourney (Midjourney)	Cloud consumer software (e.g. Google Docs)
API Access to Model	Users can send requests to the model programmatically, allowing use in external applications	Claude 3.5 Sonnet (Anthropic)	Cloud-based API (e.g. website builders such as Squarespace)
API Access to Fine-Tuning	Users can fine-tune the model for their specific needs	GPT-4o (OpenAI)	Enterprise software with customisation APIs (e.g. Salesforce Development Platform)
Open-weight: Weights Available For Download	Users can download and run the model locally	Llama 3 (Meta), Mixtral (Mistral)	Proprietary desktop software (e.g. Microsoft Word)
Weights, Data, and Code Available for Download with Use Restrictions	Users can download and run the model as well as the inference and training code, but have certain licence restrictions on their use	BLOOM (BigScience)	Source-available software (e.g. Unreal Engine)
Fully Open: Weights, Data, and Code Available for Download with no Use Restrictions	Users have complete freedom to download, use, and modify the model, full code, and data	GPT-NeoX (EleutherAI)	Open source software (e.g. Mozilla Firefox and Linux)

Key Needs for Managed Access

- Feedback and iteration on tiered framework to ensure it preserves access and benefits
- Platforms with funding to support the framework. Government should fund this work.
- Alignment on dissemination policy with journals and non-traditional publishers will be important.
- Resources and best practices for:
  - Establishing identity or legitimacy of otherwise unknown users
  - Establishing criteria for access to community tools at different levels of risk

Key Takeaways

- The Bio Funders Compact asks funders to consider biosecurity, and dissemination is a key consideration.
- Need to balance biosecurity with equitable access in exploring managed access. Striking the right balance is feasible but will take effort.
- For AI x Bio models there is a range of dissemination options between fully open source and fully closed. Publishers should consider and incorporate these options into their policies.
- Government funders (like NSF and NIH) should support tiered/managed access platforms that host AI biodesign tools.

Thank you!

Contact: nti-bio@nti.org

https://www.nti.org/area/biological/

NTI:bio

NTI
BUILDING A SAFER WORLD