National Science Advisory Board for Biosecurity (NSABB) Meeting

November 21, 2024

1:00 PM – 2:00 PM (ET)

NSABB
National Science Advisory Board for Biosecurity

New USG Policy for Oversight of Dual Use & Enhanced Pandemic Pathogen Research

- Informed by NSABB's *Proposed Biosecurity Framework for the Future of Science*
- Strengthens oversight of research posing highest risks for public health, agriculture, food security, economic security, and/or national security
- Merges existing biosecurity policies to unify and harmonize approaches for promoting benefits while mitigating risks
- Issued May 6, 2024; effective date: May 6, 2025
  - Implementation guidance: https://www.whitehouse.gov/wp-content/uploads/2024/05/USG-DURC-PEPP-Implementation-Guidance.pdf
  - FAQs: https://aspr.hhs.gov/S3/Pages/DURC-and-PEPP-FAQ.aspx

Emerging Needs: Safeguarding *in silico* Methods

- DURC/PEPP Policy forecasted needs associated with increasing evolution and use of computational models and approaches, including use of artificial intelligence (AI)
- Administration priorities include imperative of development and use of safe, secure, and trustworthy AI *(Executive Order 14110)*
  - National Security Memo (released October 24, 2024) provides further direction on appropriately harnessing artificial intelligence (AI) models and AI-enabled technologies.
  - Assessment of biosecurity concerns and benefits for AI in life sciences *(in progress, DoD sponsored National Academies Consensus Study)*
  - Baseline biosecurity practices for screening purchases of synthetic nucleic acids *(HHS funding requirements effective April 26, 2025)*
  - Publishing *in silico m*odeling and computational approaches of biological agents/organisms with biosecurity implications *(expected in 2025, NSF sponsored National Academies Workshop)*

What's Next: Roadmap for Safeguarding *in silico* Research with Potential Dual Use Concerns

For *in silico* research, computational models, and datasets, we need:

- Approaches **for identifying and assessing risks/benefits of:**
  - developing and using computational models with dual use potential
  - conducting research through computational strategies that make the design of a PEPP, novel biological agent or toxin, etc. more accessible
- Guidance **for risk mitigation** that would strengthen safety and bolster trustworthiness of such research
- Methods to **responsibly communicate research products and educate the research community** on potential misuse risks and mitigation strategies

Charge | Assessing Risks & Benefits (Phase 1A)

Recommend strategies for identifying, and options for mitigating, potential risks associated with *in silico* research, computational models [including AI models], and datasets in life sciences settings.

- Identify approaches that could result in the development of specific dual-use information or models directly enabling the design of a PEPP or a novel biological agent or toxin and conduct evaluations of AI models to measure the ability and propensity of such models to assist in specific dual-use biology tasks.
- Assess risks and benefits against clear criteria, and mitigate the risk of information hazards generated by published *in silico* research that could contribute to the design of a PEPP or novel biological agent or toxin.
- Consider how *in silico* research could enable the design, development, enhancement, or acquisition of transmissible biological agents with specific attributes (e.g., increased virulence, transmissibility, etc.).

Charge | Mitigating Risks (Phase 1B)

Outline options for promoting responsible innovation while mitigating potential risks, including methods and approaches to:

- Incorporate current and future guidelines and standards for managing misuse risks of dual use foundation models established by the National Institute of Standards and Technology into the development and release of these dual-use AI models, datasets, and research results.
- Mitigate the risk of misuse of deployed dual-use AI models, such as API-level safeguards and “Know Your Customer” practices, that could identify potential cases of misuse with minimal disruption to legitimate users.
- Select the appropriate mitigation strategies that are commensurate to the potential risk and benefits of the dual-use AI model or datasets.

Charge | Responsible Communication (Phase 2)

Explore options for promoting highest standards of transparency while safeguarding research and research outputs, including methods and approaches to:

- Responsibly share and communicate research results and datasets in repositories, preprints, and peer-reviewed publications, including decisions around model releases and “structured access” paradigms for hosting dual-use models and datasets.

- Educate the scientific community and enhance researcher and institutional awareness and oversight of the potential misuse risks and mitigation strategies.

Proposed Timeline and Deliverables

- **December:** Delivery and discussion of charge; formation of working group
- **January-May:** Data analyses, deliberations, and input
- **Summer:** Initial findings presented; discussion of additional needs
- **Fall:** Revisions to report; additional analyses, deliberations and input
- **December**: Final recommendations