Congress of the United States
House of Representatives
Washington, D.C. 20515

Anna G. Eshoo
Eighteenth District
California

October 18, 2022

Mr. Jake Sullivan,
National Security Advisor
National Security Council
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Dr. Arati Prabhakar, Director
Office of Science and Technology
Policy
1650 Pennsylvania Avenue, NW
Washington, DC 20502

Dear Advisor Sullivan and Director Prabhakar,

I'm writing to urge you to address the dual-use harm that wholly open-sourced artificial intelligence (AI) models can have with regard to biosecurity. The open-source nature of dual-use AI models coupled with both the declining cost and skills required to synthesize DNA and the current lack of mandatory gene synthesis screening requirements for DNA orders significantly increase the likelihood of the misuse of such models.[1] I urge the Administration to include the governance of dual-use, open-source AI models in its upcoming discussions with our co-signatories at the Ninth Review Conference of the Biological Weapons Convention (BWC) and to investigate methods of governance such as mandating the use of application programing interfaces (APIs).

AI has quickly become ubiquitous in many industries. .decreasing costs, increasing productivity and fostering innovation. This is increasingly true in the biotechnology and pharmaceutical industry. Technological advances in recent years have made it easier to capture and store reams of digital patient data, resulting in rich troves of genomic data, health records, medical imaging, and other patient information that AI platforms can mine to help develop drugs faster and more successfully. Companies can also use AI to model new molecules for drug discovery.

As I stated in my previous letter to you regarding the open-source, generative model Stable Diffusion, AI models released without appropriate safeguards can lead to real world harms.[2] These risks are particularly acute regarding biosecurity. The same AI models designed to assist in the design of new molecules for drug discovery can be easily transformed and directed to design new, lethal molecules. The introduction and use of AI in biotechnology and drug discovery dramatically lowers the technical thresholds in creating toxic substances or biological agents that can cause significant harm. Open-source AI is the primary route for leaning and creating new models, and the necessary datasets needed to create harmful toxins are readily available, creating significant biosecurity risks.

Researchers at the drug discovery company Collaborations Pharmaceuticals, Inc. demonstrated this recently by simply inverting their open-source machine learning model and transforming their "innocuous generative model from a helpful tool of medicine to a generator of likely deadly molecules."[3] In less than 6 hours, the AI had designed one of the most toxic nerve agents and many other known chemical warfare agents, as well as new molecules that were predicted to be more toxic than publicly known chemical warfare agents. [4]

The dual-use biosecurity risks of open-source AI models will become graver as such models provide the pieces needed to resurrect history's worst pathogens or engineer much worse. There has unfortunately already been precedent for misuse of this kind in the scientific community. In 2018, Canadian researchers reconstituted an extinct virus (horsepox) for only $100,000 using mail-order DNA.[5] In January, 2021, researchers released a paper with a step-by-step guide on how to engineer COVID-19 and make other strains in a lab.[6] Additional dual-use concerns include the synthesis of mousepox[7], the synthesis of poliovirus[8], and the generation of the 1918 influenza virus[9] in lab settings. Today's incredibly useful AI models for tasks like predicting proteins' structures will soon be succeeded by models that predict proteins' interactions, viruses' health effects, and so on. Such models could be used to not only reconstitute smallpox but engineer it to be even more communicable and deadly. Ungoverned proliferation of such AI models is untenable.

Another concern regarding ungoverned AI that is released open-source without appropriate safeguards is how it can and will be used by our adversaries. President Biden recently announced sweeping new limits on the sale of semiconductor technology to China, a step to protect the American semiconductor industry and slow the progress of Chinese military programs.[10] It would be counterproductive to limit the availability of certain technology to China while allowing the highest impact product of the technology to be transferred without government review via open sourcing.

These concerns raise the need for safe, transparent, and trustworthy AI. The Administration should encourage policymakers, academics, industry experts and scientists to engage in open dialogue about the risks these models pose and the implications of computational tools. Increased visibility into the use of these models would raise awareness about potential dual-use aspects of cutting-edge technologies. Content controls, a free content filter, monitoring of applications, and a code of conduct are several other steps industry and academia, with the coaxing of the Administration and policymakers, could take to encourage responsible science and guard against the misuse of AI-focused drug discovery. Finally, requiring the use of an API, with code and data available upon request, would greatly enhance security and control over how published models are utilized without adding much hindrance to accessibility. APIs can: (1) block queries that have potentially dual-use applications;

(2) screen users, such as requiring an institutional affiliation; and (3) flag suspicious activity. I urge you to explore this and any other viable methods within your authorities to reduce the likelihood of open-source AI models being misused for bioweapons.

AI has important applications in biotechnology, healthcare, and pharmaceuticals, however, we should remain vigilant against the potential harm dual-use applications represent for the national security, economic security, and public health of the United States, in the same way we would with physical resources such as molecules or biologics. To mitigate these risks, I urge the Administration to include the governance of dual-use, open-source AI models in its upcoming discussions at the BWC Review Conference and investigate methods of governance such as mandating the use of APIs.

Most gratefully,

Anna G. Eshoo
Member of Congress

[1] *Biosecurity for the Future: Strengthening Deterrence and Detection: Testimony before the Subcommittee on Asia, the Pacific, Central Asia, and Nonproliferation Committee on Foreign Affairs,* 117th Cong., (2021) (statement of Dr. Kevin Esvelt, Director, Sculpting Evolution Group, Massachusetts Institute of Technology), https://docs.house.gov/meetings/FA/FA05/20211208/114290/HHRG-117-FA05-Wstate-EsveltK-20211208.pdf.

[2] Anna G. Eshoo to Jake Sullivan and Alondra Nelson, September 20, 2022.

[3] Fabio Urbina et al., "Dual use of artificial-intelligence-powered drug discovery," in *2021 Swiss Federal Institute for NBC Protection* (Spietz: Spietz, 2021), https://climate-science.press/wp-content/uploads/2022/03/00s42256-022-00465-9.pdf.

[4] Ibid.

[5] Kai Kupferschmidt, "How Canadian researchers reconstituted an extinct poxvirus for $100,000 using mail-order DNA," *Science*, July 6, 2017, https://www.science.org/content/article/how-canadian-researchers-reconstituted-extinct-poxvirus-100000-using-mail-order-dna

[6] Xuping Xie et al., "Engineering SARS-CoV-2 using a reverse genetic system," in *Nature Protocols*, (2021), https://doi.org/10.1038/s41596-021-00491-8.

[7] Ronald J. Jackson et al, "Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox," *Journal of Virology* 75, no. 3 (February 2001) https://doi.org/10.1128/JVI.75.3.1205-1210.2001.

[8] Jennifer Couzin, "Active Poliovirus Baked From Scratch," Science 297, no. 5579 (July 2002) https://doi.org/10.1126/science.297.5579.174b.

[9] Terrence M. Tumpey et al, "Characterization of the Reconstructed 1918 Spanish Influenza Pandemic Virus," *Science* 310, no. 5745 (October 2005) https://doi.org/10.1126/science.1119392.

[10] Ana Swanson, "Biden Administration Clamps Down on China's Access to Chip Technology," *The New York Times*, October 7, 2022, https://www.nytimes.com/2022/10/07/business/economy/biden-chip-technology.html; Gregory C. Allen, "Choking off China's Access to the Future of AI," *Center for Strategic & International Studies*, October 11, 2022, https://www.csis.org/analysis/choking-chinas-access-future-ai.