JOHNS HOPKINS
BLOOMBERG SCHOOL
of PUBLIC HEALTH

Center for
Health Security

Summary of Biosecurity Provisions in the October 2024 National Security Memorandum (NSM) on Artificial Intelligence (AI)

November 6, 2024

The following is a summary of the biosecurity- and pandemic preparedness-relevant portions of the National Security Memorandum (NSM) on AI (October 24, 2024), titled "Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence." The NSM on AI is in fulfilment of Section 4.8 of the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (October 30, 2023).

Section 3.3(c): The Department of Commerce (DOC) shall serve as the "primary United States Government point of contact with private sector AI developers" to facilitate "voluntary unclassified pre-deployment safety testing of frontier AI models," including assessments of biosecurity risks.

Section 3.3(e)(i): Within 180 days, the AI Safety Institute (AISI) shall pursue "voluntary preliminary testing" of at least 2 frontier AI models prior to their public deployment to evaluate capabilities that might pose a threat to national security. This testing shall include assessments of models' capabilities to accelerate development of biological weapons.

Section 3.3(e)(ii)(A): Within 180 days, AISI will issue guidance for AI developers on how to "test, evaluate, and manage risks to safety, security, and trustworthiness arising from dual-use foundation models," including guidance on "how to measure capabilities that are relevant to the risk that AI models could enable the development of biological weapons."

Section 3.3(g): To reduce the biological risks that could emerge from AI, the United States Government shall "advance classified evaluations of advanced AI models' capacity to generate or exacerbate deliberate...biological threats." As part of this:

- ○ (i)
    - ● (A) Within 210 days, the Department of Energy (DOE), Department of Homeland Security (DHS), and AISI, in consultation with the Department of Defense (DOD), shall "develop a roadmap for future classified evaluations of advanced AI models' capacity to generate or exacerbate deliberate...biological threats," to be shared with the Assistant to the President for National Security Affairs (APNSA). This roadmap will include:
        - ○ The "scope, scale, and priority of classified evaluations";
        - ○ "Proper safeguards to ensure that evaluations and simulations are not misconstrued as offensive capability development";

    - “Proper safeguards for testing sensitive and/or classified information”; and
    - “Sustainable implementation of evaluation methodologies.”
  - (B) On an ongoing basis, DHS shall provide “expertise, threat and risk information, and other technical support to assess the feasibility of proposed biological... evaluations; interpret and contextualize evaluation results; and advise relevant agencies on potential risk mitigations.”
  - (C) Within 270 days, DOE shall create a pilot program to provide “expertise, infrastructure, and facilities capable” of conducting classified biological tests.
- (ii) Within 240 days, DOD, the Department of Health and Human Services (HHS), DOE, DHS, the National Science Foundation (NSF), and other agencies “pursuing the development of AI systems substantially trained on biological...data” shall support “efforts to utilize high-performance computing systems and AI systems” to enhance biosecurity, including:
  - (A) The development of screening tools for *in silico* biological research and technology;
  - (B) The creation of nucleic acid synthesis screening algorithms;
  - (C) The construction of high-assurance software foundations for novel biotechnologies;
  - (D) The screening of complete orders or data streams from cloud labs and biofoundries; and
  - (E) The development of risk mitigation strategies, such as medical countermeasures.
- (iii) All agencies that develop relevant dual-use foundation models that are public and substantially trained on biological data shall incorporate AISI’s biological safety guidance after it is published (per Section 3.3(e)), as “appropriate and feasible.”
- (iv) Within 180 days, NSF, in coordination with DOD, AISI, HHS, the Office of Science and Technology Policy (OSTP), and other relevant agencies shall “convene academic research institutions and scientific publishers to develop voluntary best practices and standards” for publishing computational biological models, data sets, and approaches, including those that use AI and could “contribute to the production of knowledge, information, technologies, and products” that could be used to cause harm.
- (v) Within 540 days, OSTP, NSC, and the Office of Pandemic Preparedness and Response Policy (OPPRP) shall develop guidance promoting the benefits and mitigating the risks associated with *in silico* biological research.