FACT SHEET: DHS Advances Efforts to Reduce the Risks at the Intersection of Artificial Intelligence and Chemical, Biological, Radiological, and Nuclear (CBRN) Threats

On October 30, 2023, President Biden signed Executive Order (E.O.) 14110 on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. The overarching goal of the E.O. was "to ensure that America leads the way in seizing the promise and managing the risks of artificial intelligence (AI)" and to establish a governance framework for the safe and responsible development and use of AI.

The Department of Homeland Security (DHS) has played a key role in implementing the E.O.. Section 4.4 of the E.O. highlighted the need "to better understand and mitigate the risk of AI being misused to assist in the development or use of CBRN threats – with a particular focus on biological weapons." Within DHS, the Countering Weapons of Mass Destruction Office (CWMD) is the office responsible for leading DHS efforts and coordinating with domestic and international partners to safeguard the United States against CBRN threats. CWMD led the development of an AI CBRN Report that evafaluated "the potential for AI to be misused to enable the development or production of CBRN threats, while also considering the benefits and application of AI to counter these threats."

The AI CBRN Report was developed through strong collaboration across the United States Government, academia, and industry. CWMD solicited insights from DHS Agencies and Offices and consulted with experts in AI and CBRN issues from the Department of Energy, private AI laboratories, academia, think thanks, and third-party model evaluators to evaluate AI model capabilities to present, mitigate, or guard against CBRN threats.

Today, DHS is releasing selected findings from the AI CBRN Report to the President.

Current Trends in AI

- The responsible use of AI holds great promise for advancing science, analyzing large complex datasets beyond human cognitive abilities, solving urgent and future challenges, and improving daily life, while potential misuse poses consequential risk requiring society-wide mitigation efforts.

- AI has already affected the way research is conducted in the physical and life sciences and will continue to do so in expected and difficult-to-anticipate ways. These AI-enabled enhancements to research can have positive and negative impacts, depending on the intent of the users and the quality of the data.

- The revolutionary pace of change in the biotechnology, biomanufacturing, and AI sectors compounds existing regulatory challenges; therefore, AI technology governance must be adaptive and iterative to respond to rapid or unpredictable technological advancements.

- The variety of publicly available AI models can help enhance physical and life science researchers' ability to ideate novel biological and chemical agents and design experiments, increase their understanding of human physiology and the interaction with proteins and toxins, and potentially troubleshoot experimental procedures encountered during experiments.

AI Misuse to Enable the Development or Production of CBRN Threats

- As AI technologies advance, the lower barriers to entry for all actors across the sophistication spectrum may create novel risks to the homeland from malign actors' enhanced ability to conceptualize and conduct CBRN attacks.

- Known limitations in existing U.S. biological and chemical security regulations and enforcement, when combined with the increased use of AI tools, could increase the likelihood of both intentional and unintentional dangerous research outcomes that pose a risk to public health, economic security, or national security.

- While each of the current frontier AI model developers have implemented a system of internal evaluation and red teaming, consistent with their participation in the White House-sponsored *Voluntary Commitments From Leading Artificial Intelligence Companies to Manage the Risks Posed by AI*, the developers' heterogenous approaches, the dual-use nature of the basic science information involved, and inconsistent access to relevant CBRN expertise, make it vital to encourage continued interaction among industry, government, and academia. Subsequent ongoing exchanges between frontier model developers and the national security and broader biodefense communities should continue, as well.

- Engagement with international stakeholders, including governments, international organizations, industry, and nongovernmental organizations, is needed to develop approaches, principles, and frameworks to manage AI risks, unlock AI's potential for good, and promote common approaches to shared challenges, in light of worldwide development and spread of AI technologies.

Benefits and Applications of AI to Counter CBRN Threats

- Integration of AI into CBRN prevention, detection, response, and mitigation capabilities could yield important or emergent benefits.

- AI tools could enhance international collaboration and communication on key efforts related to CBRN, attribution for suspected bioagent or chemical attacks and monitoring of non-state and Nation States' compliance with international agreements and adherence to arms control, nonproliferation and disarmament treaties.

- AI offers opportunities to leverage advanced analysis to bolster all lines of effort in the National Biodefense Strategy.