Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated August 3, 2026

Artificial Intelligence and Biosecurity Issues

Artificial intelligence (AI) is a term generally used to refer to computerized systems that work and react in ways commonly thought to require human intelligence. AI technologies, methodologies, and applications may benefit biological sciences research and development (R&D). For example, AI could be used in conjunction with biological design tools to enable drug design. These potential capabilities have also raised certain biosafety and biosecurity concerns. Some researchers argue that AI could be repurposed and misused to produce biological and chemical compounds of concern. Congress may continue to assess the effects of AI models and applications on biological sciences and other types of scientific R&D. Regarding potential biosecurity concerns, Congress may consider oversight mechanisms to evaluate and manage such risks, such as voluntary standards, industry-led frameworks, and regulations by federal agencies.

Introduction

AI can be used for a range of discipline-specific and broader R&D applications. An example is engineering biology, which is the application of engineering principles and the use of systematic design tools to reprogram cellular systems for a specific functional output. Use of AI in this field has enabled R&D advances across multiple application areas and industries. AI in conjunction with biological design tools can design nucleic acid sequences (e.g., deoxyribonucleic acid [DNA]), which can then be used to produce (e.g., synthesize) physical DNA. Some researchers are using AI to analyze genomic data (e.g., DNA sequences) to determine the genetic basis of particular traits, characterize proteins (e.g., determine their 3D structures), and design new chemical structures that can enable drug discovery.

More broadly, AI can be applied to scientific R&D processes. For example, AI is being deployed within autonomous laboratories (sometimes called self-driving labs or cloud laboratories) that can run experiments with minimal to no active human participation. Some researchers have suggested that these types of AI-based laboratory tools, sometimes referred to as AI scientists (e.g., science-focused chatbots), could generate new ideas and research experiments beyond their explicit tasking.

While proponents and certain developers of AI models have argued that AI will increase the speed of scientific advancements in biosciences, others have downplayed the capabilities of AI's current applications within this field. Nobel prize-winning chemist Dr. Jennifer Doudna said in a June 2026 interview regarding use of AI in biotechnology that "biology is complex" and "innovation is still really in the domain of human beings right now. … I'm not seeing chatbots coming up with a brand-new idea." AI-generated biological designs (e.g., DNA sequences) would need to be physically synthesized and evaluated to determine whether they are of any practical use or value beyond the theoretical predictions of the AI model, including evaluating predicted biosafety or biosecurity risks.

Some life sciences researchers, biotechnology companies, biosecurity/biosafety experts, and AI companies have argued that AI can be repurposed or misused in the biological sciences, raising certain biosafety and biosecurity concerns. Of note, some argue, is the ability of AI to design novel DNA sequences of concern, which, according to the National Institute of Standards and Technology (NIST), could be undetectable by current sequence screening tools.

Addressing Biosecurity Concerns of AI Models

In the United States, there currently is no single, overarching federal law governing biosafety and biosecurity with enforceable legal penalties beyond those in the Federal Select Agent Program, which covers only certain types of biological agents and toxins. Oversight of laboratory biosafety and biosecurity is exercised pursuant to a mixture of federal law, federal guidance, and self-governance, dependent on the types of experiments and biological agents being used.

On May 5, 2025, the White House issued Executive Order (E.O.) 14292, "Improving the Safety and Security of Biological Research," which directed the Office of Science and Technology Policy (OSTP) to revise or replace the 2024 *United States Government Policy for Oversight of Dual Use Research of Concern and Pathogens with Enhanced Pandemic Potential* (2024 policy) within 120 days. The E.O. also directed OSTP, within 90 days, to revise or replace the 2024 *Framework for Nucleic Acid Synthesis Screening*, which established requirements for recipients of federal funding for research related to sources of synthetic nucleic acids. According to the E.O., the new policy should "take[] a commonsense approach and effectively encourage[] providers of synthetic nucleic acid sequences to implement comprehensive, scalable, and verifiable synthetic nucleic acid procurement screening mechanisms to minimize the risk of misuse." In July 2026, the White House released the *U.S. Government Policy for Stopping High-Risk Life Sciences Research*, pursuant to the E.O. The policy replaced the 2024 policy; it did not revise or replace *the 2024 Framework for Nucleic Acid Synthesis Screening*.

AI Industry Action Related to Biosecurity

In regard to the development and use of AI generally, and AI use in biological sciences specifically, no federal legislation establishing broad regulatory authorities has

been enacted. In certain instances, industry has developed standards and self-governance frameworks addressing aspects of biosecurity as it relates to AI and the biological sciences. Government agencies have also aided in some of these efforts; for example, NIST's Biosecurity for Synthetic Nucleic Acid Sequences effort partners with stakeholders to improve current DNA screening standards and evaluates opportunities to mitigate potential risks associated with AI biodesign tools.

The International Gene Synthesis Consortium (IGSC), an industry-led group of gene synthesis companies and organizations, has developed "a common protocol to screen both the sequences of synthetic gene [purchase] orders and the customers who place them." This screening process has been implemented through industry standards and other requirements for federally funded research to address biosafety and biosecurity risks associated with nucleic acid synthesis.

In May 2026, OpenAI published a governance framework that describes the company's risk assessment and mitigation processes for cyber offense; chemical, biological, radiological, and nuclear risks; harmful manipulation; and loss of control. OpenAI has also instituted programs to investigate safeguards for advanced AI capabilities in biology, including competitions to identify jailbreaks, a process in which hackers exploit vulnerabilities in AI systems to bypass their ethical guidelines and perform restricted actions. The most recent competition invites individuals to attempt universal jailbreaks of ChatGPT's biosafety safeguards for a reward of up to $50,000.

In June 2026, Anthropic released a proposed policy framework for governments to address four risk categories of AI models: "biological weapons, offensive cyber operations, loss of control of AI systems, and automated [R&D]." The policy is divided into two parts: frontier developer obligations and societal resilience measures. Under the first part, frontier developers would test their models and mitigate for "catastrophic risks," publish their findings, and be accountable to a government agency. The second part proposes ways for "how society can prepare to withstand the threats—particularly biological and cyber—that advancing AI capabilities may accelerate or enable."

Separately, in June 2026, a group of life sciences researchers, AI companies, biotechnology developers (including some members of the IGSC), and other experts issued an open letter to Congress that read, in part, "We call on legislators to make screening of orders for synthetic nucleic acids—and the equipment needed to make them—mandatory." The responsibilities proposed in the open letter would be placed on the DNA synthesis companies and not on the biological design tools or AI models supporting those design tools.

Considerations for Congress

The use of AI in the biological sciences involves potential benefits and risks, including in the biological design capabilities of AI models. However, AI-generated biological designs may not be viable and therefore may not actually present biosafety or biosecurity risks. Given these uncertainties, Congress may consider whether current federal policies and oversight are sufficient to address potential biosecurity concerns related to the convergence of AI and biological sciences or whether to pursue further action, such as establishing new federal policies or regulatory authorities. Such actions could include advancing those efforts supported by the signatories of the open letter and discussed in the E.O. related to biotechnology industry standards (e.g., synthesis screening) and examining self-governance frameworks, such as those offered by the IGSC.

Several bills in the 119th Congress would address potential biosafety and biosecurity risks that may be enhanced by AI. For example, H.R. 3029, the Nucleic Acid Standards for Biosecurity Act, would direct federal agencies to "carry out measurement research to support the development and improvement of best practices and technical standards for biosecurity measures related to nucleic acid synthesis." S. 3741, the Biosecurity Modernization and Innovation Act of 2026, would address aspects of nucleic acid synthesis security and other biosecurity and biosafety authorities across the federal government. Addressing the impact of biotechnology and biosecurity more broadly, S. 4363, the Engineering Biology Readiness Act, would require the next biennial update of the biodefense threat assessment to include an analysis of, and recommendations relating to, the risks of engineering biology and how to modernize related biosafety, biosecurity, and biodefense authorities, regulations, and programs.

Other legislation introduced during the 119th Congress would address different aspects of the convergence of AI and biotechnology, including certain biosafety and biosecurity-related issues, biological AI data standards and data sharing, and cloud labs. These bills, individually and collectively, could support the advancements of AI and biology while also providing some safeguards.

For example, S. 4069, the AI-Ready Bio-Data Standards Act, would require the director of NIST to "establish definitions, standards, resources, and frameworks to ensure certain biological datasets are ready for use in [AI] models." S. 3952, the Future of Artificial Intelligence Innovation Act of 2026, would establish standards, metrics, and evaluation tools to support AI R&D and capacity building activities and "promote innovation in the [AI] industry." The bill also would require the examination of "safeguards and best practices to protect against unintended use of [AI] for … developing chemical, biological, radiological, nuclear, and energy-security threats or hazards." H.R. 9307 and S. 4770, the Web of Biological Data Act of 2026, would "require the Secretary of Energy to establish a centralized resource for access to data to facilitate biological research through enabling advanced computational methods such as [AI]." H.R. 7801 and S. 2676, the Cloud Labs to Advance Biotechnology Act, and similarly, S. 3468, the National Programmable Cloud Laboratories Network Act of 2025, would direct the National Science Foundation to establish a national cloud laboratory network (e.g., autonomous labs and self-driving labs).

Todd Kuiken, Analyst in Science and Technology Policy

Disclaimer