Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated November 16, 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 is being used in conjunction with biological design tools to enable drug design. These capabilities have also raised certain biosafety and biosecurity concerns. Some researchers argue that AI may 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 mechanisms to evaluate and manage such risks, including oversight of voluntary standards, industry-led frameworks, current regulations by federal agencies, or new legislation.

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. 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. These could include 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. In September 2026, Anthropic reported that individuals had used the company's AI models in ways that circumvented built-in biosafety- and biosecurity-related safeguards, including safeguards to prevent actors from certain regions of the world from accessing the AI models. The report noted, however, that the individuals are "working scientists," and the report does not "assert that they intended harm."

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.

In July 2026, the White House released the *United States Government Policy for Stopping High-Risk Life Sciences Research* (2026 policy), pursuant to Executive Order (EO) 14292, "Improving the Safety and Security of Biological Research," which, among other provisions, 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). In relation to AI, the 2026 policy applies to research that plans to create or modify a biological agent that meets the definition of dangerous gain of function and was the result of in silico research. (*In silico* refers to experiments, studies, and modeling performed via a computer versus *in vivo* [i.e., in a living cell] or *in vitro* [e.g., in a test tube].) However, purely computational research, including the development of computational models and software, which may be used to design novel forms of biological agents, is not prohibited by this policy unless it involves an entity of concern (e.g., country of concern).

Earlier in 2026, a group of life sciences researchers, AI companies, biotechnology developers, 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 group included some members of the International Gene Synthesis Consortium [IGSC], an industry-led group of gene synthesis companies and organizations.)

On November 5, 2026, the White House released its *National Policy for Nucleic Acid Synthesis Screening* (NASS). Considering impacts from the convergence of AI and biology, the NASS sets forth the U.S.-government-wide policy and establishes standards for screening orders of synthetic nucleic acids. NASS requires all recipients of federal life sciences funding to procure synthetic nucleic acids (e.g., DNA) and benchtop synthesis equipment exclusively from certified suppliers that verify the legitimacy of customers and sequences ordered. NIST is tasked with developing standards and test and evaluation protocols for screening suppliers and equipment. NASS places compliance responsibilities on the suppliers (e.g., DNA synthesis companies) and their customers and not necessarily on the developers of in silico biological design tools or AI models supporting those design tools.

AI Industry Action Related to Biosecurity

Regarding 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 some 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. NIST has also been charged with issuing the standards and test and evaluation protocols for the NASS.

The IGSC 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. How the IGSC interprets and incorporates the NASS into its processes and protocols has yet to be determined.

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 guards 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."

Considerations for Congress

AI's ability to enhance biological science research can present both benefits and risks. This can include an AI model's ability to increase, or uplift, an individual's knowledge or skills in the biological sciences. However, AI-generated biological designs may not be viable and may not actually present biosafety or biosecurity risks. The dual-use nature of biological sciences may present challenges for evaluating biosafety and 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; examining self-governance frameworks, such as those offered by the IGSC; or evaluating the effects of the 2026 policy and the NASS. Congress may also consider whether to codify such policies into law or develop alternative legislation.

Members of Congress have previously introduced bills that addressed different aspects of the convergence of AI and biotechnology, including certain biosafety and biosecurity-related issues, and biological AI data standards and data sharing. For example, legislation has been introduced to direct NIST to "establish definitions, standards, resources, and frameworks to ensure certain biological datasets are ready for use in [AI] models" (S. 4069, 119th Congress). Other legislation has proposed for NIST to establish standards and evaluation tools to support AI R&D and capacity-building activities and to promote innovation (S. 3952, 119th Congress). Congress may also consider legislation to guard against unintended use of AI for developing chemical, biological, radiological, and other threats or hazards, as proposed in S. 3952 (119th Congress). Congress may also direct the next biodefense threat assessment to assess the risks of engineering biology and how to modernize related biosafety, biosecurity, and biodefense authorities, regulations, and programs (e.g., S. 4363, 119th Congress).

These examples of legislative mechanisms, individually and collectively, could support the advancements of AI and biology while providing some safeguards that the 120th Congress may further consider. Alternatively, Congress may continue to defer to the executive branch to address the intersection of biosecurity and AI and conduct oversight on those ongoing activities, including the implementation of the 2026 Policy and NASS.

Todd Kuiken, Analyst in Science and Technology Policy

IF13269

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.