Statement before the House Committee on Science, Space, and Technology
Subcommittee on Investigations and Oversight
On Balancing Biotechnology Innovation and Biosecurity: Securing U.S. Leadership in a Global Race

Testimony of Dr. Anemone Franz

Anemone Franz
Visiting Research Fellow at the American Enterprise Institute and Postdoctoral Research Associate at the John J. Reilly Center for Science, Technology, and Values at the University of Notre Dame

September 16, 2026

Chairman McCormick, Ranking Member Sykes, and esteemed members of the Subcommittee, thank you for the opportunity to testify today on strengthening the bioeconomy and governing high-risk biological research.

I am a Visiting Research Fellow at the American Enterprise Institute and a Postdoctoral Research Associate at the John J. Reilly Center for Science, Technology, and Values at the University of Notre Dame. My work focuses on dual-use research, biosecurity, and emerging technology governance.

The US has historically led in biotechnology, and advances in this field promise unprecedented benefits for human health and well-being, the economy, agriculture, manufacturing, and national security. Sustaining US leadership in this field requires two things: continued investment in biotechnology research and development and safeguards that keep pace with changes in the underlying technology.

In my testimony, I argue that investing in both biotechnology leadership and biosecurity is more urgent now than ever and propose measures that would strengthen security without slowing legitimate research.

Three actions would help close existing gaps:

1. **Implement universal gene synthesis screening requirements.** No binding federal requirement obliges synthesis providers to screen nucleic acid synthesis orders or verify customers. Congress should establish that requirement through legislation, such as the bipartisan Biosecurity Modernization and Innovation Act.
2. **Fund pathogen-agnostic biosurveillance.** Biosurveillance investment has historically surged after each crisis and contracted afterward, and most surveillance targets known diseases rather than novel threats. Congress should provide stable, multiyear funding for detection systems that do not depend on knowing the threat in advance.
3. **Close gaps in federal research oversight.** The July 2026 Policy for Stopping High-Risk Life Sciences Research does not reach the computational design of biological agents, and binds only institutions that receive federal funding. Statutory action is required to close these gaps.

Biotechnology's Opportunities and Emerging Risks

Biotechnologies have already transformed fields such as medicine, defense, and agriculture, and their impact will increase as the underlying technologies mature. However, the same research and technologies that produce these benefits also create risk. For example, research intended to understand dangerous pathogens to develop countermeasures can generate knowledge that could be misused to make those pathogens more lethal or transmissible. This “dual-use dilemma” makes it particularly difficult to safeguard biotechnologies without slowing beneficial research.

Biological threats are not new. In addition to natural outbreaks, instances of laboratory accidents and deliberate misuse of biological agents have been well documented.[1][2] What has changed in recent years, however, is the pace of scientific and technological progress. Together with falling costs, barriers that have historically made engineering biology difficult are eroding. AI, in particular, is changing what is possible in biotechnology while also introducing risks with little precedent. Advanced AI models could reduce the level of expertise required to manipulate and potentially weaponize biological agents. This concern has even been raised by the companies that are building these models.[3][4]

AI model capabilities are advancing fast and often outpace the safeguards meant to contain them. The July "Hugging Face incident" illustrates this problem. In this incident, several of OpenAI’s models, operating under reduced safeguards during internal cybersecurity evaluations, circumvented the controls meant to restrain them and, coordinating through unauthorized channels, “compromised parts of OpenAI’s internal research infrastructure and Hugging Face’s systems.”[5]

While much attention has focused on large language models, misuse risk is not limited to this model type. Biological AI models, trained on biological data rather than natural language, offer a different set of capabilities and risks. In a recent *Science* publication, researchers at Stanford and the Arc Institute reported that they had trained such models to generate functional viral genomes from scratch.[6] Sixteen of the sequences the models produced yielded viable, infectious viruses.[7] The potential to design novel pathogens creates a new risk profile for two reasons. Because these pathogens may not resemble anything found in nature, they may not trigger existing safeguards. Furthermore, if optimized for their potential to cause harm, they may exceed the lethality or transmissibility of anything natural selection has produced.

These risks are substantial, but safeguards needed to address them have been identified, and most can be implemented without constraining the research on which the field's benefits

[1] https://www.cdc.gov/anthrax/bioterrorism/index.html
[2] https://www.thelancet.com/journals/lanmic/article/PIIS2666-5247(23)00319-1/fulltext
[3] https://www.anthropic.com/threat-intelligence-report-september-2026#biological-misuse-sep-26
[4] https://openai.com/index/preparing-for-future-ai-capabilities-in-biology/
[5] https://openai.com/index/hugging-face-incident-and-the-road-ahead/
[6] https://www.science.org/doi/10.1126/science.aec2657
[7] https://www.science.org/doi/10.1126/science.aec2657

depend. The recommendations that follow set out where federal effort would be most valuable.

Maintain US Biotechnology Leadership

The United States leads in biotechnology, but sustaining that position requires continued investment in the underlying research, the skilled workforce, and the manufacturing sector. In its 2025 report, the National Security Commission on Emerging Biotechnology warned that the biotechnology sector has not been treated with the same strategic urgency as semiconductors or artificial intelligence, even as competition with China has intensified.[8] Federal research, regulation, manufacturing, and workforce development are each handled in isolation rather than as parts of one system, producing a landscape that is difficult to navigate.[9] Supply chains are a further point of exposure. Feedstock additives, which are used in most biomanufacturing processes, are one example. Chinese suppliers account for nearly all global production, and a disruption in supply could bring dependent facilities to a standstill.[10]

Congress should ensure adequate funding for biotechnology research and development, invest in the technical workforce, coordinate these efforts across agencies, and reduce dependence on foreign suppliers for materials that have no domestic alternative.

Secure Access to Synthetic Nucleic Acids

Engineering a biological agent is a complex process requiring a series of steps and access to a range of materials. Some of those steps are difficult to avoid, and identifying and securing these chokepoints is an effective way to reduce risk. A particularly salient chokepoint is access to synthetic nucleic acids (DNA and RNA). Nucleic acids are a key ingredient for life sciences research. Researchers can order custom sequences from commercial providers. To date, no binding federal requirement obliges those providers to screen the sequences they are asked to synthesize or to verify their customers' legitimacy. Safeguarding DNA synthesis has instead relied on industry-led voluntary screening, coordinated largely through the International Gene Synthesis Consortium, which represents a majority of global commercial synthesis capacity.[11] The principal obstacle to stronger safeguards is therefore not industry resistance but the absence of standardized requirements.

Both the executive branch and Congress have moved to close this gap. Executive Order 14292 in May 2025 directed the Office of Science and Technology Policy (OSTP) to incorporate enforcement mechanisms into the existing framework and to develop a strategy for achieving comprehensive screening in non-federally funded settings.[12] Earlier this year, a bipartisan group of legislators introduced the Biosecurity Modernization and Innovation Act,

[8] https://www.biotech.senate.gov/wp-content/uploads/2026/07/NSCEB-Full-Report-%E2%80%93-Single-Pg-%E2%80%93-July-2026.pdf
[9] https://www.biotech.senate.gov/wp-content/uploads/2026/07/NSCEB-Full-Report-%E2%80%93-Single-Pg-%E2%80%93-July-2026.pdf
[10] https://assets.carnegieendowment.org/files/Fluegel_Biomanufacturing.pdf
[11] https://genesynthesisconsortium.org/
[12] https://www.whitehouse.gov/presidential-actions/2025/05/improving-the-safety-and-security-of-biological-research/

which would require mandatory screening for all synthesis providers selling to US customers, establish conformity assessment systems with auditing and adversarial testing, and direct a government-wide assessment of biosecurity authorities to streamline oversight.[13] Enacting it would be a significant step toward establishing these safeguards as a common standard.

Uniform screening standards would strengthen, not disadvantage, domestic industry. Providers meeting US security standards would gain a competitive advantage, while those unwilling to comply would lose access to the world's largest synthesis market.[14] Because the requirements would apply to all providers serving US customers, including Chinese firms seeking access to that market, standards established here would function as global standards.

Prevent Biological Misuse of AI Models

Federal oversight of AI models with biological applications depends largely on voluntary commitments by industry and on conditions attached to federal funding, and it is applied unevenly across different classes of models.[15] Frontier developers of large language models conduct biosecurity evaluations and implement mitigations, but no federal requirement obliges them to conduct these evaluations or to report their results.[1617] Biological design tools receive considerably less scrutiny, despite posing risks that are arguably more consequential.[18]

Congress should close this gap without extending oversight further than the risk requires. Only a narrow subset of models requires additional attention, and identifying that subset is the first step. The Center for AI Standards and Innovation (CAISI) conducts pre-deployment evaluations of frontier models, including for biological risk, but does so through voluntary agreements with developers.[19] Congress should make these evaluations a requirement rather than a voluntary arrangement, and should fund and direct CAISI to define capabilities of concern for biological AI models.[2021] The definitions should be revisited regularly as capabilities advance and should prioritize capabilities that could enable, accelerate, or simplify the creation of pathogens capable of causing a pandemic.[2223] As evaluation

---

[13] https://www.congress.gov/bill/119th-congress/senate-bill/3741/text
[14] https://www.precedenceresearch.com/dna-synthesis-market#%3A%7E%3Atext%3DThe%20market%20is%20highly%20competitive%2Cmarket%20in%20the%20coming%20years
[15] https://www.belfercenter.org/sites/default/files/2026-08/Belfer_Deterrence%20by%20Resilience_3.2_Digital%20Final.pdf
[16] https://openai.com/index/preparing-for-future-ai-capabilities-in-biology/
[17] https://www.anthropic.com/research/biorisk
[18] https://journals.plos.org/ploscompbiol/article?id=10.1371/journal.pcbi.1012975
[19] https://www.nist.gov/caisi
[20] https://www.csis.org/analysis/opportunities-strengthen-us-biosecurity-ai-enabled-bioterrorism-what-policymakers-should
[21] https://democrats-energycommerce.house.gov/sites/evo-subsites/democrats-energycommerce.house.gov/files/evo-media-document/12.17.2025_oi-hearing_witness-testimony_pannu.pdf
[22] https://www.csis.org/analysis/opportunities-strengthen-us-biosecurity-ai-enabled-bioterrorism-what-policymakers-should
[23] https://journals.plos.org/ploscompbiol/article?id=10.1371/journal.pcbi.1012975

methods developed for large language models do not transfer to models trained on biological data, distinct approaches will be needed. For models in that subset, evaluation should be required before deployment, and results should be linked to clearly communicated, pre-specified thresholds and corresponding mitigations.[24] This includes withholding concerning data from training, restricting access to verified users through secure channels as appropriate, and government risk-benefit review.

Strengthen Dual-Use Research Governance

Working with dangerous pathogens entails a certain level of risk. The goal of oversight is not to eliminate that risk but to determine how much risk is acceptable, under what conditions, and who can make that judgment. That determination is difficult because of the dual-use dilemma, and because outcomes of an experiment can be difficult to know in advance. Only a narrow subset of work with dangerous pathogens warrants heightened scrutiny, while most pathogen research should proceed with standard safeguards.

Federal policy has made significant progress on dual-use research governance in recent years. In May 2025, Executive Order 14292 restricted federal support for dangerous gain-of-function research where adequate oversight was lacking, suspended other federally funded work of that kind pending a new framework, and directed stronger oversight, enforcement, and screening measures for high-risk research.[25] That follow-on policy, the United States Government Policy for Stopping High-Risk Life Sciences Research, was released in July 2026 and applies to every institution and investigator receiving federal funds for life sciences research.[26] The new policy abandons static pathogen lists in favor of a risk-based approach, prohibits rather than reviews seven categories of dangerous gain-of-function research, and establishes an independent review body for borderline cases.[27]

These policies could significantly strengthen oversight. The move to a risk-based approach is particularly valuable. List-based oversight covers only known threats. As biotechnology draws on components from multiple organisms, the species of origin has become an unreliable indicator of risk — and as the *Science* study noted above shows, AI can help design viral genomes from scratch.[2829] Lists are also slow to update, which is a serious limitation when the underlying technology is advancing at an unprecedented pace.

The policy does, however, place considerable weight on judgment. Investigators and institutions must now predict whether proposed work could produce significant negative societal consequences for public health, agriculture, the economy, national security, or the environment, and several of the policy's central terms are open to differing interpretation.[30]

---

[24] https://journals.plos.org/ploscompbiol/article?id=10.1371/journal.pcbi.1012975
[25] https://www.whitehouse.gov/presidential-actions/2025/05/improving-the-safety-and-security-of-biological-research/
[26] https://www.whitehouse.gov/wp-content/uploads/2026/07/USG-Policy-for-Stopping-High-Risk-Life-Sciences-Research_July-2026.pdf
[27] https://www.whitehouse.gov/wp-content/uploads/2026/07/USG-Policy-for-Stopping-High-Risk-Life-Sciences-Research_July-2026.pdf
[28] https://journals.sagepub.com/doi/full/10.1089/hs.2022.0109
[29] https://www.science.org/doi/10.1126/science.aec2657
[30] h, however, placesttps://www.whitehouse.gov/wp-content/uploads/2026/07/USG-Policy-for-Stopping-High-Risk-Life-Sciences-Research_July-2026.pdf

Institutions must screen their entire life sciences portfolio, including non-federally funded work, and the funding and legal consequences attached to uncertain definitions may lead to overconservative interpretations to protect the institution.[31] This may result in chilling effects on legitimate research.

This concern can be addressed by working closely with the people tasked with implementing the policy. Scientists and biosafety officers will need to apply these policies, and their cooperation will determine whether they function as intended. Implementation guidance should set out clearly how to identify research within the policy's scope and distinguish good-faith disagreement from deliberate concealment.

Two gaps in the current framework require legislative action. First, the policy does not cover purely computational research unless it involves an entity of concern.[32] The policy directs OSTP to convene an interagency group to monitor developments at the intersection of biology and artificial intelligence. Given how quickly these tools are advancing, computational design of biological agents should also be brought under binding oversight. Second, the policy reaches only federally funded research. Institutions without federal funding are encouraged, not required, to adopt equivalent procedures, and the policy itself notes that statutory action is needed to reach all US entities.[33]

Build Detection and Attribution Capacity

Detecting and identifying a novel biological threat as early as possible is crucial. Early detection makes it possible to develop and deploy countermeasures quickly and to contain a threat before it reaches catastrophic scale. After detection, investigators must determine whether the agent arose from a natural spillover, a laboratory accident, or a deliberate act. If it proves to have been engineered, investigators must trace its origins to a specific laboratory, country, or actor.

The COVID-19 origins debate illustrates the cost of being unable to answer these questions. Nearly seven years after the virus was first detected, its origins remain contested. This uncertainty has eroded public trust, strained international relations, and left significant security questions unresolved. Detection and attribution capabilities cannot be built during a crisis. They must be established and maintained in advance to be available when needed.

To improve detection capabilities, three changes are particularly important. First, detection must be pathogen-agnostic. Most surveillance focuses on specific, known diseases and therefore may miss novel biological threats. Second, funding must be sustained. Biosurveillance investment has historically surged after each crisis and contracted in its aftermath, leaving capacity to erode before the next threat emerges. Third, the United States should sustain and increase investment in monitoring capacity and genomic data-sharing infrastructure with international partners. Pathogens do not respect borders, and a serious

[31] https://www.whitehouse.gov/wp-content/uploads/2026/07/USG-Policy-for-Stopping-High-Risk-Life-Sciences-Research_July-2026.pdf
[32] https://www.whitehouse.gov/wp-content/uploads/2026/07/USG-Policy-for-Stopping-High-Risk-Life-Sciences-Research_July-2026.pdf
[33] https://www.whitehouse.gov/wp-content/uploads/2026/07/USG-Policy-for-Stopping-High-Risk-Life-Sciences-Research_July-2026.pdf

biological threat may first appear outside the US. Detection capacity abroad therefore can provide crucial advance warning that domestic surveillance alone cannot.

Reliable attribution would strengthen biosecurity in several ways: It can deter actors who realize that their designs could be traced back to them, enable accountability through legal or diplomatic action, and inform outbreak response by revealing critical properties of the engineered pathogen.

Emerging technologies have the potential to advance attribution considerably, and machine learning approaches have produced promising results.[34] There has been periodic interest in advancing these technologies. DARPA launched a Bio-Attribution Challenge earlier this year that aims to develop tools to determine the origins of engineered pathogens.[35] However, competitions alone will not realize this technology's full potential. Sustained government investment and private-sector collaboration are needed.

Data is a further constraint. Current systems are trained largely on plasmids deposited in academic repositories, which offer limited accuracy when applied to pathogen genomes and exclude the Biosafety Level 3 and 4 laboratories that pose the greatest risk.[36] Building adequate and secure training datasets, including from high-containment facilities, is a precondition for advancing attribution technologies.[37]

Technical capability alone is not sufficient for reliable attribution. A high-confidence finding is only as useful as the system that must act on it, and establishing consensus on what counts as evidence, how it is weighted, and how it informs decisions is as essential as the underlying science. Attribution will also rarely rest on a single source. A mechanism is needed to bring together the different forms of evidence, such as forensic analysis, epidemiological data, intelligence, and records held by commercial providers, into a single assessment. These capabilities take years to build and must be in place before they are needed. Congress has an essential role in establishing and sustaining that investment.

Conclusion

The United States does not have to choose between leading in biotechnology and governing it responsibly. Both, however, require active investment: in the research, workforce, and manufacturing capacity that sustain American leadership, and in safeguards targeted narrowly enough to address real risks without impeding legitimate science.

I would like to thank the Subcommittee for its leadership in addressing these critical questions, and I look forward to hearing your questions.

---

[34] https://www.nature.com/articles/s41467-022-35032-8

[35] https://www.darpa.mil/research/challenges/bio-attribution?utm_source=linkedin&utm_medium=social&utm_campaign=bio-attribution-challenge&utm_term=march-26&utm_content=bto-challenge-announcement

[36] https://thebulletin.org/2025/12/tracing-engineered-biothreats-with-ai-forensics-five-steps-to-improve-attribution/#post-heading

[37] https://thebulletin.org/2025/12/tracing-engineered-biothreats-with-ai-forensics-five-steps-to-improve-attribution/#post-heading