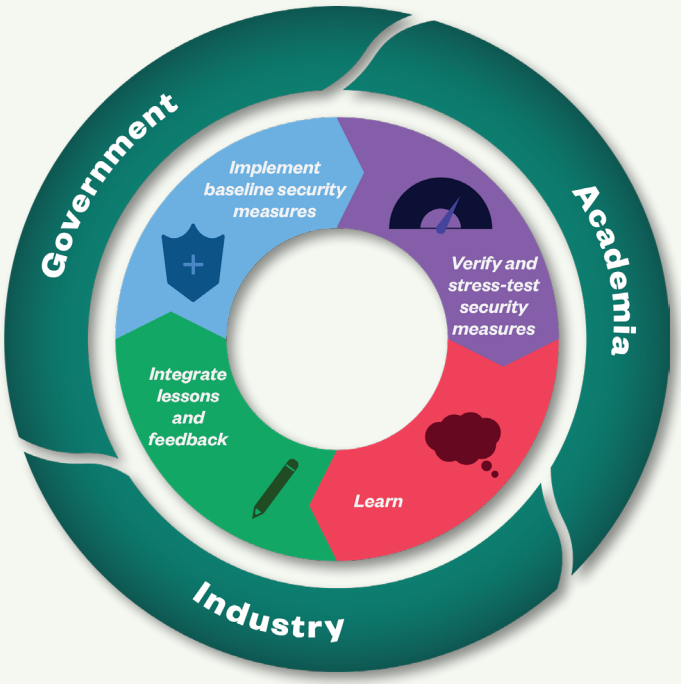
Strengthening Gene Synthesis Security

Desired Outcomes and Capabilities

A new approach to gene synthesis security

Gene synthesis, the process of creating physical genes based on digital sequence data, is critical for growing the U.S. biotechnology industry. The industry currently relies on voluntary security guidance from government[1] and industry,[2] which may be an inadequate approach to prevent harms while ensuring global competitiveness.

Moving forward, Congress should designate an entity to employ an iterative governance approach to secure gene synthesis. This approach would include engaging stakeholders, implementing a base level of security, conducting exercises to verify implementation and test the limits of security systems, extracting lessons learned, and integrating those lessons into improved security practices (see figure). The designated entity would regularly report progress towards outcomes with the appropriate legislative oversight committee.



The described approach would position the U.S. Government to lead by example in synthesis security. Focusing beyond customer and sequence screening, this approach would include the ability to respond to both the needs of implementers and changes in the technical and geopolitical landscapes. It incorporates an ability to rapidly detect and respond to security, ethical, and other concerns.

This concerted ability to improve over time would build resilience toward threat vectors, assist with the regular updates required in the Office of Science and Technology Policy's Framework for Nucleic Acid Synthesis Screening,[1] strengthen confidence in providers and manufacturers, and enable continued scientific and economic growth in the industry. Conversely, legislation in this space that does not create adaptive and responsive security capabilities runs the risk of being ineffective, overly burdensome, or even creating perverse incentives that undermine both security and economic goals.

This white paper presents outcomes and capabilities that policymakers could incorporate into future approaches to governance. Notably, this paper leaves open whether the Federal Government or a designated entity, such as a public-private partnership, is best positioned to coordinate with gene synthesis providers and manufacturers toward meeting these outcomes and capabilities. Examples to draw upon include Information Sharing and Analysis Centers (ISACs),[3] the National Institutes of Standards and Technology (NIST) Artificial Intelligence Safety Institute Consortium (AISIC),[4] and Aviation Safety Information Analysis and Sharing (ASIAS).[5]

Desired Outcomes and Capabilities

Implement baseline security measures:

- **Pilot security governance with stakeholders:** The Federal Government would incentivize the design and piloting of governance ideas with a representative selection of stakeholders before rolling them out across the industry.
- **Implement baseline security standards for gene synthesis providers and manufacturers:** Gene synthesis providers and manufacturers that are based in, or ship to, the United States would adhere to baseline security standards, including, but not limited to, existing sequence and customer screening techniques.[1]

Verify and stress-test security measures:

- **Engage in exercises to verify baseline adherence to security standards:** Joint exercises between the Federal Government, gene synthesis users, synthesis providers, manufacturers, and screening service providers can both build and verify adherence to

standards beyond a self-attestation statement. A federal agency or designated entity could design and regularly conduct such exercises. To keep pace with advances, this agency or entity should be adequately resourced and staffed with sufficient expertise (such as a federal agency having appropriate hiring authorities).

- **Engage in exercises to improve synthesis security robustness:** To better understand the limits and costs of current standards, even when properly implemented, the same agency or entity could design and conduct regular stress-testing exercises with select stakeholders on a voluntary basis.

Learn from reporting, research, and other information sources:

- **Report concerning activity on a tiered basis:** Currently, it is difficult to obtain data on the adequacy of designations of "sequences of concern," and existing policy allows providers and manufacturers to determine their own thresholds for reporting concerning activity. Many set thresholds so high that few reports happen. The moment of gene synthesis is an opportune point to collect this data. Not all sequence orders nor all customer or synthesis-related activity (e.g. cyber vulnerability detection) should elicit the same level of concern. The Federal Government would establish the risk thresholds or criteria that would trigger tiered reporting, with the lowest tiers being the easiest to report, perhaps even in an automated fashion. Tiered reporting requirements would provide early warnings of suspicious activity without unduly burdening industry or users. These requirements would also enable cross-industry analysis of risk assessments and enable stakeholders to provide data for revising criteria of concerning activity. The Federal Government should consider the perspectives of users and foreign governments when deciding who should manage this reporting system, the costs and liabilities of reporting, and any subsequent required actions.
- **Establish points of contact between relevant government entities and providers or third-party vendors:** The relevant government entities would maintain working relationships with the providers, manufacturers, and third-party vendors tasked with flagging an order or reporting an incident, as well as with the entity responsible for collecting and maintaining the reporting system.[1]
- **Invest in ensuring effective implementation and continually improving capabilities for identifying and addressing security concerns:** Improved synthesis security capabilities, such as security-by-design[6] and screening systems, will enable more responsible development of emerging biotechnology. The Federal Government would establish dedicated research efforts to catalyze innovation in these capabilities, either internally or by fostering private engagement through funding or prizes.

Integrate lessons and feedback:

- **Establish a multisectoral forum for feedback:** A forum involving members across the synthesis community would help ensure the synthesis security oversight is meeting the needs of all stakeholders. The forum would review topics related to risk thresholds and the validity and implementation of security measures, such as characteristics of sequences of concern, security standards, global trends, and other relevant matters.
- **Iterative security standards development:** The designated agency or entity would regularly analyze input from such a multisectoral forum, lessons learned from exercises, reporting data, and knowledge of emerging technical capabilities to draft updated security standards.

Sources

1 Office of Science and Technology Policy. "Framework on Nucleic Acid Screening."
2 International Gene Synthesis Consortium. "Harmonized Screening Protocol v2.0."
3 National Council of ISACs. https://www.nationalisacs.org
4 National Institute of Standards and Technology. "Artificial Intelligence Safety Institute Consortium (AISIC)."
5 Federal Aviation Administration. "Aviation Safety Information Analysis & Sharing (ASIAS)."
6 Nuclear Threat Initiative. "Biosecurity-by-Design to Safeguard Emerging Bioeconomies."

For any questions about this white paper, or related work at the National Security Commission on Emerging Biotechnology, please contact us at ideas@biotech.senate.gov.

Staff at the National Security Commission on Emerging Biotechnology authored this paper with input from the expert Commissioners. The content and policy options in this white paper represent ideas that the Commission is considering as we move toward official policy recommendations.