Workshop report

Genome Engineering and Biosecurity: Industry Practices, Resources, and Opportunities

Organizers: Sarah R. Carter, Science Policy Consulting; Beth Vitalis, Inscripta; Deanna M. Church, Inscripta; Kathryn R. Brink, Stanford University; Megan J. Palmer, Stanford University

Introduction

Safeguarding biosecurity will be critical to the advancement of genome engineering tools, platforms, and applications. Minimizing the risk of malicious misuse or unintended harmful outcomes of these capabilities and technologies will require engagement with stakeholders across the community to develop common strategies, principles, guidance, and perhaps, in some cases, technical tools. To initiate collaboration on these topics in the context of microbial genome engineering, Inscripta spearheaded a virtual, discussion-based workshop in collaboration with Stanford University on November 8, 2021. Collectively, the 27 workshop organizers and participants (listed below) have diverse expertise, views, and roles in the genome engineering community, with over half actively involved in industry. Prior to the workshop, the organizers held small scoping discussions with many of these participants as well as representatives from the U.S. government, which helped sharpen the focus and achieve actionable insights. The objectives of the workshop were to:

- Identify common biosecurity concerns for genome engineering capabilities.
- Begin to define future-proofed technical tools and practices needed to help assess or mitigate the risks that may arise from genome engineering capabilities.
- Strategize a community-based path forward to develop biosecurity best practices and define the broader community that should be engaged in these discussions.

This report outlines the key findings from the discussion at this workshop. Although there was much discussion of risks, strategies, and resources for identifying and mitigating risks, and gaps and needs for biosecurity, this initial workshop did not seek to gain consensus or to prioritize among potential hazards or needed resources. However, there was a clear desire among participants for the development of an inclusive community to facilitate dialog and action on these topics. Further discussions are needed to generate some level of consensus on what types of risks should be considered under different circumstances, who should conduct biosecurity screening or evaluations, and what types of resources or tools are most needed. Into the future, ongoing collaboration can support development and improvement of best practices and shared resources. Given the rapid pace of advancement of genome engineering tools, the establishment of such a biosecurity group is urgently needed so that standards and practices can be developed and promulgated as the industry matures.

Publication Date: February 2022

Key findings

Wide range of considerations for risks related to genome engineering

Participants raised concerns about a wide range of hazards that may arise from genome engineering capabilities and products. Some were relatively simple (e.g. editing of a toxin gene) while others included levels of context and complexity related to whole genomes (e.g. genome recoding), whole organisms (e.g. engineering a harmless strain of *E. coli* into a harmful strain), or ecological interactions in a complex environment (e.g. harmful persistence of an organism or its genes in the human microbiome or in the outside environment). Participants also discussed a variety of circumstances in which risks might arise in the context of their companies or products, including unintended harmful outcomes and intentional misuse by customers. The context in which genome engineering tools or products are used is important; even widely distributed, generalizable tools (e.g. CRISPR constructs) could be misused to cause harm. The diversity of companies and business models represented at the workshop, including both those that develop genome engineering tools and capabilities as well as those that use those tools to generate novel strains, contributed to the broad scope of risks and circumstances that were identified.

Existing industry approaches and resources for identifying and mitigating risks

Industry participants had considered, informally or formally, ways to identify and mitigate risks that may arise from their genome engineering tools and products, and in workshop discussions, they shared some approaches and resources that they use. Many of the companies work collaboratively with customers and have access to customers' design parameters, which mitigates the potential for intentional misuse of their genome engineering capabilities. Some workshop participants mentioned technical approaches to strain development such as careful selection and screening of initial strains, barcoding, other methods for tracking, and use of kill switches. Discussion and differing opinions about the value of these approaches highlighted the need for further engagement to identify good and best practices. Examples of available resources included screening tools to determine if DNA sequences are found in regulated pathogens or are predicted to enhance pathogenicity (e.g. ThreatSEQ and tools funded by IARPA's Fun GCAT program such as SeqScreen) and regulatory guidance documents related to the use of genetically engineered organisms in the environment and related to food safety (e.g. FDA and EPA guidance, international allergen database). However, because these resources were not designed for evaluation of genome engineering projects or products, they often require some adaptation or interpretation when used in these contexts.

Challenges, gaps, and resources needed to identify and mitigate risks

The discussion on approaches and resources to identify and mitigate risks moved quickly and repeatedly to challenges and gaps in available tools and knowledge. Development of additional resources is critical. The workshop discussion highlighted the need for:

- **Research and technical advances to address the challenge of working with biological complexity** at the level of the whole genome, organism, and even ecosystem. Some specific areas included how to: predict potential harmful outcomes (including ontologies and typologies of concerning signals as well as contexts); track organisms and survey for harmful outcomes; identify potential outcomes that will be difficult to reverse; and track iterative changes to strains over time (even across multiple projects, genome engineering tools, and perhaps personnel). Although some of these topics are large and complex, even imperfect tools that can flag a genome engineering project or strain for closer scrutiny can be helpful in an industry context.

- **Best practices that include business considerations.** These include incentives for companies to conduct biosecurity screening, ways of securely tracking the chain of custody of strains (including sequences, bioinformatic analyses, and risk assessments), conducting assessments while protecting customer data, clarity about company liabilities if and when a risk is realized, and clarity about customer screening and customer intent, including when customer screening is necessary and how to adequately screen customers. Given the diversity of companies and business models in the genome engineering community, these discussions are likely to be wide-ranging.

- **An overarching resource that would list risks that companies should consider.** Such a document could also include any available resources that could be used to identify or mitigate each risk, and would help elucidate specific gaps in knowledge, best practices, or tools.

- **Resources for communication and education about biosecurity** that could be used in interactions with customers, policy makers, investors, the general public, and even within companies.

- **Reliable databases**. Many of the DNA screening resources already available depend on publicly available databases such as those maintained by NCBI, and these resources should be strengthened and secured as critical bioinformatic infrastructure.

Need for an ongoing group focused on biosecurity and the genome engineering industry

There was broad agreement among workshop participants that a new, ongoing group or forum is needed with a focus on biosecurity and the genome engineering industry. Such a group would allow for discussion, collaboration, and standards-setting for risk identification and mitigation in the industry. It could also serve as a focal point for education and outreach within the industry and for a wide range of stakeholders. This discussion drew on lessons learned from the International Gene Synthesis Consortium (IGSC), and there were several suggestions for how to align this activity with the IGSC and other efforts related to genome engineering, including BioMADE, Genome Project-write, and Engineering Biology Research Consortium (EBRC). The discussion also highlighted the value of including academic and other non-industry participants. Although the genome engineering community is diverse, there was support for a unified group; participants pointed out that many risks related to genome engineering can arise regardless of the particular genome engineering approach that is used or the circumstances in which an organism is intended to be used. Discussion points related to establishment of an industry-focused genome engineering biosecurity group included the need for:

- **Sustained funding and development of organizational principles for governance**, membership, and operation.

- **A process to prioritize action**, including development of different resources, given the diversity of risks most relevant to different applications and the diversity of biosecurity approaches that might be considered by companies.

- **Strategies to overcome challenges related to sharing of data** among companies for biosecurity assessments and learning opportunities (e.g. case studies). For example, lists of denied sequences or projects requiring further scrutiny can be developed (and have been developed for pathogen and toxin sequences), but these lists or determinations are sometimes considered information hazards and so are difficult to use and share. Allowable sequences or projects that have been considered and cleared are also helpful, but these are often closely tied to customer data and so are considered proprietary.

- **Methods for communication with government stakeholders** as potential funders and technology developers. Similarly to the IGSC, this group could also help inform policy development for biosecurity oversight of genome engineering capabilities.

Conclusion

The genome engineering community is diverse in its tools and approaches to engineering, products that are made, and business models that are followed. This diversity requires wide-ranging discussions on approaches and resources to identify and mitigate the potential for unintended harmful outcomes or opportunities for malicious misuse of genome engineering tools or products. The participation and enthusiasm of participants at this workshop demonstrates that the industry community is eager to have these challenging discussions and to make progress toward improved biosecurity. The organizers are grateful for their time and contributions (both at the workshop and, for many, pre-workshop interviews), and look forward to ongoing collaboration.

Participants

Zack Abbott, ZBiotics
Jean-Claude Abboud, Arzeda
Kate Adamala, University of Minnesota
Andy Baltus, Addgene
Craig Bartling, Battelle
Patrick Boyle, Ginkgo Bioworks
Peter Carr, MIT Lincoln Lab
Dianna DeVore, Inscripta
James Diggans, Twist Bioscience
Steve Evans, BioMADE
Ian Fiddes, Inscripta
Michal Galdzicki, Arzeda
Fernando Garcia, Amyris
Nathan Hillson, Berkeley National Lab
Connor Hoffmann, Stanford University
Peter Lee, Ginkgo Bioworks
John W. K. Oliver, ZBiotics
Neeraj Rao, Battelle
Sarah Richardson, MicroByre
Tom Slezak, KPATH Scientific, LLC
Amy Schwartz, Genome Project-write
Krista Ternus, Signature Science, LLC