Synthetic Biology Industry Practices and Opportunities for Biosecurity and Potential Roles for the U.S. Government

Sarah R. Carter, Ph.D., Principal, Science Policy Consulting LLC
Diane DiEuliis, Ph.D., Senior Research Fellow, National Defense University

Table of Contents

** The views and opinions expressed in this report are those of the authors and do not specifically reflect those of the individuals who contributed perspectives to the project, National Defense University, the Department of Defense, or the Defense Threat Reduction Agency, which funded the study. The authors assume full responsibility for the report and the accuracy of its contents.

Publication Date: November 2019

Introduction

The goal of synthetic biology is to make biology easier to engineer. Over the past several years, synthetic biology tools and capabilities have advanced rapidly, enabling a new generation of biotechnology products that is expanding beyond medicine and agriculture to fuels, food, materials, and other sectors (NASEM 2015, NASEM 2017). To support development of these products, the synthetic biology industry has grown to include a wide range of companies that offer diverse products and services. The U.S. "bioeconomy" is now a significant contributor to the U.S. economy (Carlson 2016, Bioeconomy Capital 2018) and investment in the synthetic biology industry continues to grow (Schmidt *et al*. 2019).

In addition to harnessing economic growth, the U.S. government, including the Department of Defense (DoD), has a high level of interest in leveraging technologies developed using synthetic biology. The DoD sees many areas where these tools can help protect the warfighter and support military operations (Carter and Warner 2018, DiEuliis 2018). At the same time, the rapid rise of enabling synthetic biology capabilities has caused some concern among policymakers who worry that these tools could be misused by nefarious actors to cause harm (NASEM 2018, Mauroni 2018). The international nature of synthetic biology technology development also raises broader concerns about economic competitiveness, control and security of data and intellectual property, and potential vulnerabilities of the U.S.-based industry, which may impact national security. To better understand these biosecurity issues, we undertook a project to map the synthetic biology industry, including its products and customers. We also explored current business practices within the industry and began a multi-stakeholder discussion of how these practices can be developed to mitigate the potential for misuse and to protect capabilities.

This project includes input from over 50 individuals, gathered through interviews, discussions during the workshop, and, in some cases, less formal conversations. Ideas and perspectives were also collected at widely attended events such as Syn Bio for Defense (held in Arlington, VA, in September 2018 and 2019) and SynBioBeta conferences (held in San Francisco, CA, in October 2018 and 2019). We spoke to 37 industry representatives from companies actively engaged in developing synthetic biology tools and capabilities, venture capitalists, and non-profit entities that substantially contribute to the industry landscape. These included companies that provide synthetic DNA, gene or genome editing tools and services, bioinformatic tools, protein and organism design services, laboratory robotics, and other biotechnology products and services. In addition to industry, we spoke to 19 policy experts and government representatives (including individuals from DTRA, other DoD offices, HHS, NIH, DHS, FBI, OSTP, and DoC). On May 23–24, 2019, we convened a workshop that included both industry and policy representatives for an in-depth discussion of industry practices and biosecurity. (A full list of Project Contributors is listed in Appendix B, and the Workshop Agenda is found in Appendix C.)

This report summarizes discussions with industry representatives about the current and future structure of the synthetic biology industry, perspectives on potential misuse and vulnerabilities of synthetic biology tools and capabilities, and business practices to prevent misuse of tools and to protect industry assets. Based on these perspectives and workshop discussions, this report identifies areas where the collaborative development of best practices may support the industry and enhance biosecurity. Potential roles for the U.S. government in supporting, guiding, convening discussions on, and overseeing different aspects of biosecurity in the synthetic biology industry are also included. Critically, this project identified an urgent need for establishment of an ongoing venue for in-depth discussion of biosecurity issues that includes U.S. government and synthetic biology industry stakeholders.

In addition to informing policy makers within the U.S. government, this document is intended to serve as a resource to the synthetic biology industry in evaluating biosecurity issues, including the potential for misuse and the vulnerabilities of these tools and capabilities. Although this report attempts to reflect a wide range of viewpoints and perspectives, and input on its conclusions and recommendations was widely solicited, this is not a consensus document.

The Synthetic Biology Industry Ecosystem

Because the synthetic biology industry is characterized by the tools and capabilities that make biology easier to engineer, it includes a wide range of products and services that support biotechnology development in many different economic sectors (see Figure 1). The industry is best described as an ecosystem of companies that are diverse, interconnected, and interdependent. Companies that provide synthetic DNA or genome editing tools form a critical foundation for the rest of the industry, supporting other businesses that add their own technologies and services (horizontal bars shown in Figure 1). The end products from the vertical sectors often represent the convergence of many different synthetic biology capabilities. Others have described this interconnected nature of synthetic biology companies in similar terms, as an ecosystem (Rejeski 2017) or a technology "stack" (Canine 2018, Schmidt *et al.* 2019) that supports biotechnology innovation. The structure of this synthetic biology ecosystem has implications for biosecurity and the misuse of synthetic biology (Carter and DiEuliis 2019).

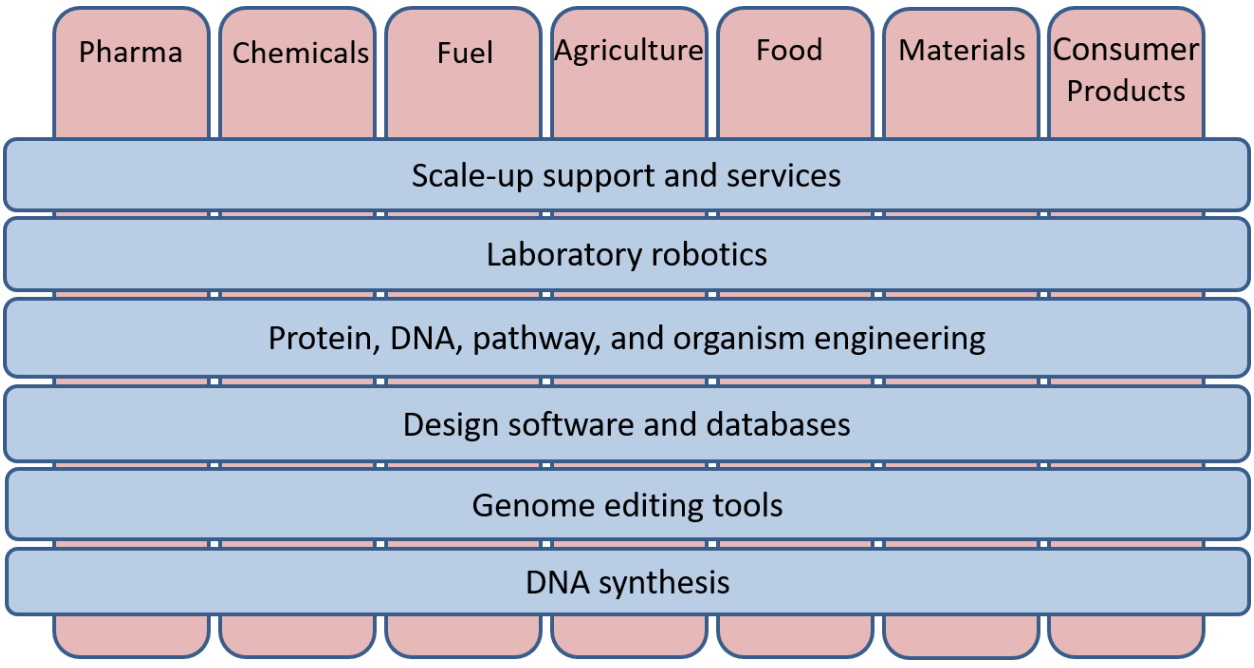

Figure 1: The Synthetic Biology Industry Ecosystem: horizontal tools and capabilities supporting a range of different vertical economic sectors (reproduced from Carter and DiEuliis 2019).

The industry supports a wide range of business models within this ecosystem. Figure 1 serves as a map that can help describe some of these models. Some companies focus on a single horizontal capability that they offer in support of many different types of biotechnology products. Others, such as Ginkgo Bioworks, have incorporated many of these horizontal capabilities to offer more integrated services. Still others have found a niche providing a specific type of tool (e.g. protein design services) for a single sector (e.g. pharmaceuticals). Synthetic biology companies are very interconnected and interdependent, often working together to leverage one another's strengths and build new capabilities (for examples, see Hyde 2019a and Friedman 2019a). Many larger, more established companies within the vertical economic sectors, such as Corteva Agriscience, have worked to bolster synthetic biology capabilities within their organizations. Industry representatives emphasized that mastering the integration of a variety of tools and capabilities is necessary for innovation and success in synthetic biology on an industrial scale, and that such integration requires customization.

Synthetic biology tools and capabilities (the horizontal bars in Figure 1) highlight the digital nature of synthetic biology. At its core, synthetic biology seeks to take digital information (DNA sequence) and transform it into predictable biological function. Nearly every part of synthetic biology development now depends on digital tools such as databases, other bioinformatic resources, and software. The vastness of DNA sequence data and the complexity of biological function makes the application of machine learning and artificial intelligence to synthetic biology an obvious choice. There has been much interest and investment in recent years in companies that integrate machine learning and artificial intelligence into synthetic biology capabilities, including for protein design, organism engineering, laboratory robotics, and scale-up prediction and operation. Companies often compete on the quality of their databases, how customizable their tools are, and how well integrated their algorithms can be into operations. Industry participants also noted that digitally controlled robotics is an expanding area in all aspects of the industry, allowing faster and more reproducible construction and testing of biological components.

Although synthetic biology is often defined by the tools and capabilities that make biology easier to engineer, knowledge specific to each sector (the vertical bars in Figure 1) is just as critical for product development in the industry. Synthetic biology companies often distinguish themselves by developing their capabilities into sector-specific tools such as libraries of CRISPR guide RNAs, relevant databases for machine learning, or tools compliant with FDA's "current good manufacturing practices" for pharmaceutical production. Because these sectors and their products are very diverse, critical considerations such as regulatory oversight, requirements for scale-up, and public perceptions vary widely. In some sectors, regulation drives decision-making about which organisms are used, with strong preferences in the U.S. for those that have a "history of safe use" for chemical or enzyme production (for EPA) or are "generally recognized as safe" for food (for FDA). Internationally, there are a wide variety of regulatory approaches and differences in public perceptions that determine opportunities for specific types of products. For example, China has recently indicated that it may ease its restrictions on genetically engineered organisms, including production of some genome edited crops (Cohen 2019), while Europe has reinforced its strict oversight of genetically modified organisms, including those that are genome edited (Callaway 2018). More discussion of the international aspects of the industry is below.

There are a few issues that reach across much of the synthetic biology industry. The need for skilled and talented workers, particularly those capable of integrating multiple types of tools, was cited as an ongoing challenge. Scale-up of products to commercial scale is a critical step in every sector, from production of gene therapy vectors to microbial fermentation to crop planting. In addition to technical

hurdles (e.g., ensuring that a microbe behaves similarly in a bioreactor as it does on the benchtop and engineering the end-to-end process), geographical challenges were often cited, including the need to move benchtop innovations from research labs in dense cities to areas where larger facilities can be built, that are nearer to feedstocks, or where seeds can be planted. Within the U.S., this often means moving from areas with strong synthetic biology talent pools (particularly San Francisco or Boston) to more rural parts of the country. Although this shift can be a challenge for companies established on the coasts, it may also create opportunities for rural America (Cumbers 2019). Some companies have reported strong economic pressure to move production overseas, particularly to Asia. In making the leap to commercial scale, synthetic biology companies often develop new partnerships, expanding the scope and complexity of the synthetic biology industry ecosystem.

Funding models for the synthetic biology industry have changed in the past few years, with increased investment from venture capital sources (Schmidt *et al.* 2019). Many industry representatives reported that much of the increase in the past decade has come from sources that have traditionally focused on information technologies and digital tools, with limited experience in biotechnologies. Foreign investment, particularly from China, increased in recent years, but new U.S. government rules related to the Committee on Foreign Investment in the U.S. (CFIUS) may decrease such investment (Hancock and Kuchler 2019; see more below). The past ten years has also seen an increase in incubators, which provide lab space and support for small, early-stage companies trying to show initial viability. In addition to incubators in biotech hubs like San Francisco and Boston, incubators are increasingly found in other parts of the U.S. and internationally, including in China (Hoyt 2017). These incubators highlight the fact that many new synthetic biology companies can establish proof-of-principle for their innovations with small amounts of funding, in contrast to more traditional biotechnologies (Friedman 2019b).

Biosecurity, Misuse, and Vulnerabilities

Like a biological ecosystem, the synthetic biology industry can be evaluated and discussed in different ways and from multiple perspectives. Here, we focus on aspects of the industry ecosystem that are likely to have the greatest implications for biosecurity, liability, vulnerabilities, and the potential for misuse. These include access to tools and capabilities, the digitization of biology, and the international nature of synthetic biology development.

Access to Tools and Capabilities

There is a strong cultural theme in some parts of the synthetic biology community toward democratization, empowering individuals to participate in genetic engineering, and the use and availability of open-source tools. This theme has its roots in early synthetic biology efforts that aimed to expand access to genetic engineering, for example, by establishing libraries of genetic "biobricks" (Morton 2005) and developing communities of students and others to see what they could do. The International Genetically Engineered Machines (iGEM) competition, the rise of Do-It-Yourself biology (DIYBio), and community labs are part of this movement, and these organizations generally take biosafety and biosecurity very seriously (iGEM 2019, Aharony 2019). The U.S. government has contributed to this community with tools that support a wide range of users, including with foundational resources like GenBank, established in 1982 (NCBI 2019), and with newer efforts such as the Department of Energy's Joint Genome Institute, a user facility for synthetic biology (JGI 2019), and KBase, an open bioinformatic tool for synthetic biology (Arkin *et al.* 2018). In addition to governmental,

academic, and non-profit entities, there are some companies in the synthetic biology industry today that actively espouse this ideal and focus on expanding access to tools. A few, such as the laboratory robotics company OpenTrons, have received investment from venture capital and other sources.

Access to synthetic biology tools and capabilities has raised concerns about biosecurity and misuse for many years, and a range of concerns were raised in discussions for this project (see Box 1 on Potential Misuse). However, the tools that are currently most widely available, including synthetic DNA, genome editing constructs, basic bioinformatic tools, and simple laboratory robotics (e.g., an OpenTrons benchtop pipetting machine), increase the capabilities of their users in limited ways. Industry representatives participating in this project emphasized that innovative synthetic biology projects still require significant tacit knowledge, experience, and resources. Even so, many (though not all) companies that provide these increasingly accessible products conduct some form of customer screening to help prevent misuse of their products (see more on customer screening, below).

Access to the most powerful synthetic biology tools and capabilities is generally limited to companies and organizations that can afford significant investment. Examples include: nanomaterials to selectively deliver genome editing constructs to specific tissues (offered by Ligandal); proteins designed *de novo* for specific functions (Arzeda); massively parallel, barcoded genome editing (Inscripta), organism design facilitated by artificial intelligence (Asimov or TeselaGen), massively parallel mutagenesis and directed evolution (EnEvolv), or supported by robotics and large-scale, experimentally validated databases of enzyme function (Ginkgo); large-scale, integrated laboratory robotics with machine learning capabilities (Synthace or LabGenius); and scale-up support powered by data analytics and machine learning (Riffyn or Zymergen).

The companies that provide these tools also provide valuable services and expertise that allow these synthetic biology capabilities to be applied in a customized way and integrated into product development. These companies generally have just a few customers (often, large businesses) and establish on-going, collaborative, and legally binding relationships with each customer or, in some cases, work with other companies on joint ventures with equal footing. Industry participants reported that a very large portion of recent investment in synthetic biology has gone into companies with this more service-oriented type of business model rather than those with a simple transfer of goods from business to customer. This arrangement has significant benefits for biosecurity as it would be very difficult for a nefarious actor to make use of these capabilities without drawing attention. In sectors with significant regulatory requirements (such as pharmaceuticals and some types of agriculture), product development is more expensive, and assets are even more closely held.

A nefarious actor would also have to contend with the fact that many tools developed for commercial purposes may be sector-specific, as discussed above, and not easily transported between sectors. For example, services and tools for massively parallel genome editing, organism engineering, or scale-up of microbial fermentation are often customized and optimized for variants of *E. coli*, *S. cerevisiae,* and other commonly used microbes. Such capabilities may have limited utility to a nefarious actor seeking to engineer a pathogenic organism or grow it at scale.

Still, the pace of development and advancement in synthetic biology continues at an impressive rate, with private investment that continues to rise (Schmidt *et al.* 2019). Genome editing using CRISPR was reported, commercialized, and became universally available within just a few years, and other innovative new tools may do the same. As time goes on, many of the capabilities currently considered to be “advanced” will become more commonplace and more widely available. For both DNA synthesis and

genome editing, the arrival of a new generation of benchtop devices may also complicate discussions of access to capabilities. Several companies are working to develop benchtop DNA synthesis and assembly machines that will go beyond short, single stranded oligonucleotides (e.g. Evonetix, DNA Script, and Nuclera), and one benchtop DNA assembly machine is already on the market (the BioXP from SGI-DNA). Inscripta recently launched the Onyx platform, a benchtop device that allows massively parallel, barcoded genome editing of genes and genomes of interest (LeMieux 2019). Both the BioXP and the Onyx platform require ongoing communication with the company that allows oversight of how they are used. Although the companies that are currently developing these benchtop devices are generally aware of the potential for misuse and are committed to securing these capabilities, it is unclear how these tools will shape the industry in the future. It will be important for the U.S. government, industry representatives, and others interested in the potential for misuse of synthetic biology to continue to assess and discuss what types of actors have access to what types of technologies.

Box 1: Potential Misuse of Synthetic Biology Tools and Capabilities

Most industry representatives that participated in this project believed that identifying and mitigating risks related to misuse of synthetic biology tools was a worthy endeavor. However, in discussing the potential for misuse, it is essential to first acknowledge that these tools are overwhelmingly used to develop useful products, overcome challenges, and promote social good. There were a few industry representatives that considered it wrong to single out synthetic biology tools for additional scrutiny, when all types of tools are potentially dual use. Some also believed that dissemination of these tools as widely as possible was itself a laudable goal that would support grassroots innovation and improve societal outcomes, including those related to biosecurity.

Industry representatives that contributed to the discussion about misuse provided a very wide range of potential concerns and scenarios for harm that range from pandemic pathogens to misuse with lower impacts to economic and ethical damages. These included:

- Using synthetic DNA to create harmful viruses or other infectious agents
- Designing proteins, genome editors, and/or vectors targeted to harm humans, plants, or animals
- Engineering organisms to produce novel toxins and/or to produce toxins within the body
- Developing novel products that unintentionally enhance existing pathogens or agents
- State actors could more easily make bioweapons (pathogens)
- A start-up company could get funding and use it for illicit activities
- Pathogen detectors (or other bio-based sensors) could be tricked with false positives/negatives
- Biohackers or researchers could edit the DNA of themselves or others (including germline edits)
- Researchers or others could release a gene drive organism without authorization
- Companies could be hacked, resulting in lost intellectual property and/or corrupted data
- Companies could make a product that is ethically dubious or has unintended ethical outcomes

These concerns include many that are well established and have been described previously by the National Academies and others (NASEM 2018, NASEM 2016, Kirkpatrick *et al.* 2018) and some for which there are already examples, such as biohackers using CRISPR constructs on themselves (Zhang 2018) and researchers conducting ill-advised germline editing on humans (Cyranoski 2019a). Given the wide range of capabilities and types of products that the synthetic biology industry represents, it is not surprising that the types of concerns that were raised varied substantially.

One concern that was raised repeatedly was that of public perceptions: would a high-profile incident of misuse (e.g., a CRISPR vector used to harm someone) cause a backlash against the industry? Several industry representatives worried that newer synthetic biology capabilities could be considered "scarier" than better-known risks, and that the media and organizations opposed to synthetic biology (or older generations of genetically modified organisms) may create a panic based on concerns with only minimal impacts. Such a scenario could lead to new restrictions on synthetic biology, causing economic damages and lost opportunities for useful tools and applications.

The Digitization of Biology

As described above, synthetic biology is increasingly a digital enterprise, with digital tools, databases, and software playing an important role in nearly every company and product. This digitization has important implications for biosecurity, including the potential for misuse of synthetic biology tools and the types of vulnerabilities these companies are likely to have. Synthetic biology companies are generally very well aware of cybersecurity threats, and often use secure computational resources for databases, software, and other key intellectual property. However, the interconnected nature of the industry ecosystem creates challenges as those resources need to be shared or integrated into the operations or products of other companies, sometimes as part of complex supply chains. Protection of data is even more challenging as the synthetic biology industry becomes increasingly international. As the U.S. bioeconomy grows, U.S. companies and the federal government (including the DoD) are likely to use and depend on synthetic biology tools and capabilities. Data protection will cease to be simply a problem for individual companies and will become a systemic issue that could impact national security.

Data security risks in synthetic biology are similar to those in other industries with digital assets. More specific to synthetic biology (and related fields) are risks that may arise because cyber intrusions into these companies may have biological outcomes, a concept sometimes called "cyberbiosecurity" (Murch *et al.* 2018) or digital biosecurity. Such risks might include, for example, hacked laboratory robotics that synthesize toxin DNA or tamper with microbial fermentation, sensors that fail to indicate pathogens or other contamination, and databases with substituted or corrupted DNA sequences. Benchtop DNA synthesis or genome editing machines could be hacked to bypass biosecurity or oversight measures. For companies that develop personalized medicines or cell therapies, these cyberbiosecurity risks may include direct harm to human health or risks to patient privacy. Best practices for cybersecurity can help protect against these risks. However, as companies and others come to depend on bioinformatic resources and digitally enabled tools, extra care must be taken to ensure that they are not compromised.

Synthetic Biology as an International Enterprise

The synthetic biology industry is increasingly international. Even small U.S. start-up companies often have customers in other countries, and many established companies have production facilities overseas and supply chains that reach around the world. These relationships provide great business opportunities for these companies, but also complicate issues related to biosecurity and the potential for misuse. Customer screening for customers in other countries can be particularly difficult. In some areas of the world, oversight and physical security are lacking, leading to the potential for stolen organisms (along with IP) and other technologies. Data security is also more challenging in these contexts.

In the U.S., these issues often come up in the context of China. China has been aggressively and strategically pursuing synthetic biology development within China, particularly supporting research for biomedical applications (Kazmierczak et al. 2019, Hyde 2019b), while the U.S. government lacks strategic planning for these technologies (DiEuliis 2018). This imbalance raises concerns about economic competitiveness, but also broader issues about leadership, including how technologies will be developed and who will have oversight (Gronvall 2015, Choulika 2018). These issues are already coming to the fore with China racing ahead in many genome editing applications (Cohen and Desai 2019) and the controversy surrounding a Chinese scientist's use of CRISPR to edit the germline of human embryos (Cyranoski 2019a).

In addition to investments in Chinese synthetic biology, industry representatives participating in this project routinely noted that Chinese interest in U.S.-based companies has increased over the past several years. This interest includes significant venture capital investment in early stage companies, though new rules under CFIUS have begun to limit this investment (Hancock and Kuchler 2019). Several industry representatives pointed out that it is often difficult for an entrepreneur to know where investment money originated due to the structure of venture capital and other funds, with limited partners often unnamed.

For products and services sold within China, Chinese investors often require that U.S. companies share data and intellectual property with Chinese partners. A number of companies have taken this deal, even with some loss of data security. At the same time, China has strict controls that prevent human genetic data generated in China from moving overseas (Cyranoski 2019b). These issues can have major implications for synthetic biology companies trying to serve Chinese customers or whose supply chains include Chinese data, services, or partners. When considered across the entire industry, many U.S. officials believe this asymmetrical loss of data and intellectual property to China constitutes a national security risk.

Developing Industry Best Practices

The interviews and workshop undertaken for this project identified several areas where business practices can be developed to improve biosecurity. These include customer screening to prevent misuse, determination of potential risks, and data security and intellectual property safeguards. In each of these areas, companies described a variety of practices and approaches. These practices range from informal (e.g. to determine potential risks, employees at a company may discuss over coffee ways that their products could be misused) to formal (e.g. for data security, lawyers at larger companies have developed contracting language to prevent improper data sharing with third parties). By sharing experiences and comparing outcomes in a non-competitive or pre-competitive environment, best practices in each of these areas can be distilled and disseminated. Although industry participants in this project recognized the importance of discussing biosecurity and the potential for misuse, they repeatedly emphasized that biosecurity considerations were not a priority for the industry overall, with very little attention paid to the topic by investors and in industry venues. Many of the practices discussed here have benefits beyond biosecurity, increasing the potential that companies and investors will find them worthwhile.

Customer Screening

Customer screening is the process of ensuring the legitimacy of customers who will make use of products or services. It includes a wide range of practices, from determination that an otherwise unknown customer has a valid credit card to full collaboration with a customer, including sharing of data, materials, intentions, and goals. Figure 2 includes examples of practices at many different levels of customer screening.

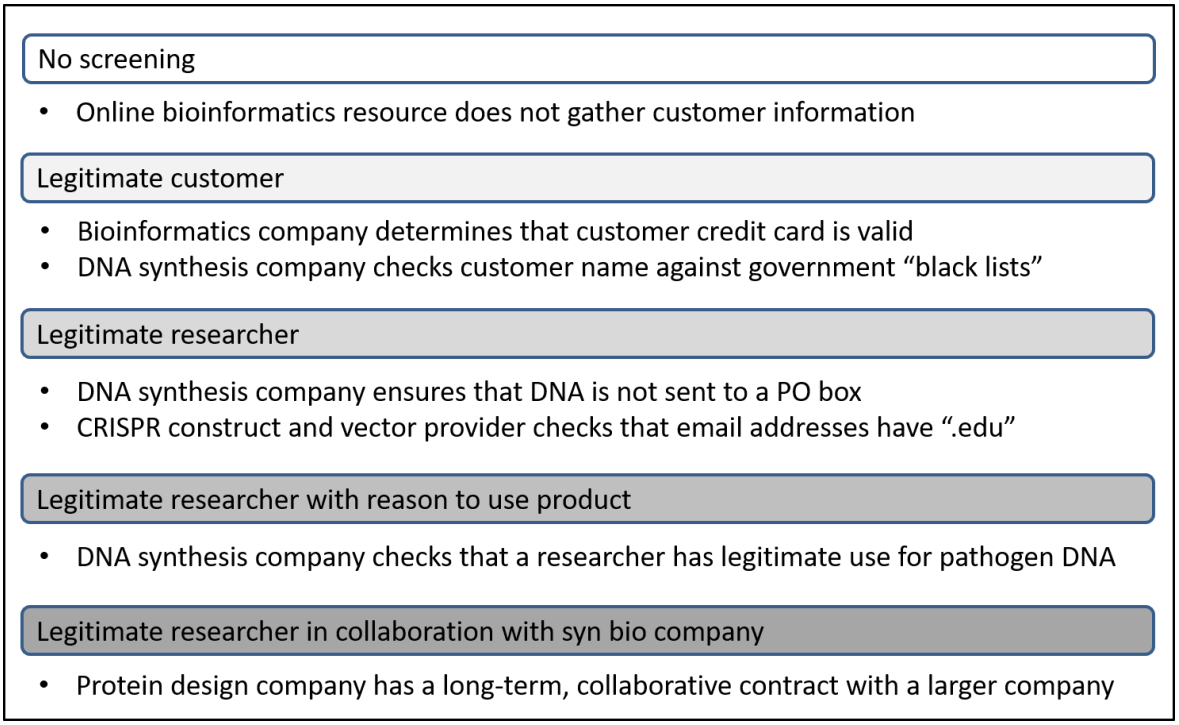

Figure 2: Different Tiers of Customer Screening with Examples

The question of what it means to be a legitimate user is a complex one, and it necessarily depends on the technology that the customer is pursuing. As described above, many businesses have advanced tools and operate collaboratively with just a few customers. These include, for example, protein design companies that work to develop superior enzymes or novel proteins for chemical or pharmaceutical companies; organism engineering companies that work collaboratively with companies seeking to produce flavorings and fragrances; and laboratory automation businesses that work with their customers to automate workflows and incorporate sensors and machine learning algorithms to improve output. These collaborative models were chosen in each case for business and economic reasons but have clear advantages for building trust, sharing goals and intentions, and ensuring that synthetic biology capabilities are being used in legitimate ways.

Some products, such as synthetic DNA and simple genome editing tools, are cheaper and businesses that provide them have many more customers. In these cases, customer screening is more challenging. One key hurdle for these companies is that it is difficult to determine what level of customer screening is appropriate for each type of product. There is virtually no guidance on how to determine the end user of a tool or capability or what constitutes a legitimate user, and companies have generally made these determinations on their own. These challenges are compounded because how a product will be used or misused depends on the intent of the customer, which can be difficult or impossible to discern; these interactions depend on qualitative determinations of trustworthiness. A broader discussion and a better understanding of how these decisions have been made across different types of technologies and companies would be valuable (also see the section on determination of potential risks, below).

In some parts of the industry, customer screening practices have become relatively well established. Most DNA synthesis providers have incorporated customer screening into their operations in

compliance with the Screening Framework Guidance for Providers of Synthetic Double-stranded DNA, issued in 2010 by the U.S. government (HHS 2010). This guidance calls on DNA providers to ensure that customers are legitimate users of synthetic DNA (with more stringent follow-up screening for customers ordering pathogen or toxin DNA or DNA sequences that endow or enhance pathogenicity). These companies determine that a customer is a legitimate user primarily by checking government blacklists and ensuring that those who order DNA are affiliated with an established institution (such as a research institution or company). Addgene, a non-profit repository and distributor of research tools, including CRISPR constructs and vectors, also has an established customer screening protocol. In this case, customers are screened to ensure that they represent non-profit or academic institutions so that Addgene can meet its obligation and mandate as a provider of tools for research purposes only. Although this customer screening is not conducted explicitly for biosecurity purposes, it safeguards the technologies in a similar way as the screening conducted by DNA providers. The U.S. government maintains multiple watch lists of entities and individuals that are either barred from receiving certain exports from the U.S. or require additional scrutiny (Export.gov 2019). These lists are already used by some synthetic biology companies, though practices vary in how they are used and how ambiguous hits are resolved.

Customer screening at a variety of levels (see Figure 2) is already a cornerstone in the synthetic biology industry for preventing misuse of widely accessible tools and capabilities. The U.S. government could support these practices by issuing new guidance or by broadening the existing HHS Screening Framework Guidance to include customer screening for a broader range of synthetic biology companies (not just DNA providers). Even absent official guidance, given that the synthetic biology industry has already developed some experience with customer screening, best practices should be collected and disseminated. These should include not only different standards for what might constitute a legitimate user for different types of technologies, but also considerations such as at what stage customers are screened, who within the company conducts screening, how those people are trained, and how uncertain findings are pursued and decided. Ongoing opportunities to share new tools and discuss challenges would further ensure that a broader range of synthetic biology companies can effectively incorporate customer screening into their business practices. A collaborative venue for these discussions could also allow cross-industry identification of individuals or entities that have a history of responsible use of synthetic biology technologies and those that may pose some risk.

Determination of Potential Risks

There are many ways that synthetic biology could be misused by a nefarious actor to cause harm, and many industry representatives participating in this project described ideas for how their products or services could be misused (though a few did not believe that their tools could uniquely cause harm). These determinations are generally made informally, as there is no guidance on how to think through these issues or what to do with any identified potential risks.

There is already significant guidance, policy, and even regulations from the U.S. government related to pathogens, including the Select Agent Regulations (FSAP 2017), policies and guidance related to Dual Use Research of Concern (NIH 2019) and Potential Pandemic Pathogens (HHS 2017), and export control (BIS 2017). However, most synthetic biology companies are focused on application areas that do not fall under these frameworks. Indeed, many are unaware of these lists, criteria, and restrictions (synthetic DNA providers are a notable exception). Furthermore, many of the potential risks identified by industry practitioners are not related to pathogens (see Box 1, above). Beyond pathogens, there is a significant number of guidance documents related to risk assessment for specific types of products undergoing

regulatory approval, both within the U.S. and internationally. These often cover a wide range of potential risks, including hazards to human, animal, and plant health and the environment, and are likely to be very useful for some synthetic biology companies that focus in specific sectors, particularly those developing products with intended uses in the environment. However, such guidance does not address intentional misuse.

A collaborative process across industry to develop best practices could incorporate awareness of pathogen-related frameworks and regulatory risk assessments but could also ask broader questions. These questions might include, for example: Could pathogens, pathogen DNA, or pathogen DNA sequences be introduced into your workflow without your knowledge? Could your technology be misused to hurt someone? Would this harm just one person, a few people, or could it spread? Does your tool overcome significant barriers for your customer? If a nefarious actor or company used your capability, what could they do with it? Possibilities for mitigation of identified potential risks could include, for example, changes to business practices (e.g., screening of customer-provided samples and DNA sequences) or flagging specific types of orders for more stringent customer screening or oversight. Common approaches and standards for benchtop DNA synthesis and genome editing devices could also be discussed and developed. Many companies already consider these types of questions and work to mitigate identified potential risks, but there have been very few opportunities to share and compare those practices. Convening discussions of this type would need to be done carefully and include measures to prevent and mitigate information hazards (i.e., the spread of information on ways tools could be misused). Guidance from the U.S. government on these broader questions could help drive productive conversations.

Data Security and Intellectual Property

Cybersecurity best practices are followed by most synthetic biology companies to secure intellectual property, computer systems, and company data. However, there are several challenges to data security that the synthetic biology industry faces beyond the level of day-to-day operations. Many of these could be addressed in part by awareness and dissemination of best practices.

A key challenge is that of foreign investment, particularly from China. As mentioned above, there is an increasing interest in biotechnology and synthetic biology from Chinese investors, including investments in U.S.-based companies. In some cases, these arrangements can lead to a loss of data, data security, and intellectual property to China. Given the fact that U.S. companies and the federal government itself may come to depend on these capabilities, many U.S. officials believe that such a loss may have implications for national security. Recent updates to regulations requiring review of foreign investments in U.S. companies by the Committee on Foreign Investment in the United States (CFIUS) reflect this concern. Since changes to CFIUS procedures were announced in late 2018 (Barker *et al.* 2018), awareness within the synthetic biology industry and among venture capital investors has increased, and Chinese investment in U.S. biotechnology companies has decreased dramatically (Hancock and Kuchler 2019, Narayanan 2019). However, guidance and best practices on how to comply with CFIUS and to protect U.S.-based data and intellectual property have not been developed. Additional clarity from CFIUS officials and a venue for discussion of these topics would be beneficial to the entire industry.

Synthetic biology companies face challenges when considering how to best secure their intellectual property even without international investment, and they employ a wide range of approaches to patenting and trade secrets. In discussions at the workshop, it was noted by multiple industry representatives that there are very few legal precedents for how synthetic biology intellectual property

will be considered by the courts. There is significant case law related to the pharmaceuticals, manufacturing, and software algorithms, and many companies have followed these precedents. However, these ill-fitting models do not capture the range of products and services developed by synthetic biology companies, and industry representatives report uncertainty on best practices (navigating two Supreme Court cases was flagged as particularly vexing: *Alice vs. CLS Bank International* [Nouri 2018] and *Association for Molecular Pathology v. Myriad Genetics* [Klusty and Weinmeyer 2015]). As the industry matures and successful models are developed, information on different approaches should be shared.

The increasingly interconnected nature of the synthetic biology industry, as described above, also creates challenges for data protection. A single biotechnology product may incorporate tools and capabilities from multiple companies. These relationships are often formalized in contracts and subcontracts, but it can be difficult to manage (or sometimes, even to identify) all the components and companies within that product's supply chain. This creates opportunities for a security breach and misappropriation of the product or data related to the product. Some synthetic biology companies, particularly larger ones with more complex supply chains, have developed legal and contracting practices to manage these risks. These issues are not specific to synthetic biology, and best practices from other industries (such as software development and cell phone manufacturing) could also be explored and applied. Technical solutions can also help: some synthetic biology companies have begun to develop APIs (application programming interfaces) for securely communicating with partnering companies. Expanding such practices through technical development and dissemination of existing solutions can both ensure data security and facilitate those productive interactions.

Next Steps and the Role of the U.S. Government

The synthetic biology industry and the U.S. government share a desire for a healthy ecosystem of companies that allows it to thrive while minimizing biosecurity risks. It has been widely acknowledged that the future bioeconomy in the U.S. has tremendous potential in many arenas, including biomedicine, agriculture, energy, and environmental sustainability (NASEM 2017), in addition to applications most relevant to DoD (Carter and Warner 2018, DiEuliis 2018). The bioeconomy also stands to be a formidable component of the U.S. economy, and as such has related national security importance. Throughout this project, there was much discussion of the role of the U.S. government and ways that it could support the industry.

A critical theme throughout this project was the need for a standing, multi-stakeholder venue where the synthetic biology industry and the U.S. government have regular opportunities to discuss biosecurity issues and best practices. The workshop held as part of this project showed the value of these discussions, with some topic areas generating more interest than anticipated, and both industry and U.S. government participants emphasizing the need for further interaction.

Such a group could help inform biosecurity practices within the industry as well as U.S. government policy related to synthetic biology. Although development of best practices, including those discussed above, could be pursued within the industry alone, U.S. government involvement would broaden their reach. In addition to providing critical information and perspectives to some discussions, a more formal venue would help raise the profile of the issue and encourage industry participation. Current *ad hoc* discussions are helpful to those industry representatives who participate, but a more authoritative group may be better able to disseminate ideas and conclusions to companies and others with fewer

resources or limited awareness. Because the synthetic biology industry is still very young, with new companies being established at a rapid pace, a centralized venue that can provide ideas and key considerations to new entrants would be helpful, even in the absence of formal guidance or consensus best practices.

In addition to providing information and perspective to U.S. government stakeholders, a group of this type would also provide critical insight into potential policy development, funding priorities, and other government activities. Project discussions yielded several suggestions for how U.S. government funding could be leveraged to improve biosecurity. For example, biosecurity-specific grants could be awarded to companies and others that would like to conduct red-teaming exercises or those that have already identified vulnerabilities or the potential for misuse and would like to develop capabilities to secure their technologies. A community of practice based on these funded activities could be tapped to help disseminate best practices. Such considerations could also be incorporated into existing funding mechanisms, such as SBIR grants and grants and contracts for training or early-stage research. Support in funding calls for security features that are built into new technologies, from bioinformatic resources to organisms, would help drive innovation in this space. There was some discussion about the role of the U.S. government, and the DoD in particular, as a key customer for and co-developer of some of these technologies, with a suggestion that DoD be thoughtful and explicit about its security needs for these technologies. A venue for ongoing discussions could help generate and shape partnerships in support of technology development.

Project discussions generated several ideas from industry participants where additional guidance from the U.S. government or guidance co-developed by industry and the U.S. government might be useful. These include guidance on: customer screening and how to determine if someone is a legitimate user; how to conduct a biosecurity risk assessment for different types of technologies (e.g., are there CRISPR guide RNAs we should look out for? Are specific types of data particularly vulnerable?); and how to consider issues related to CFIUS. Guidance relevant to the broader synthetic biology industry could be incorporated into existing guidance, such as the HHS Screening Framework Guidance, or could be developed as separate guidance. Industry representatives also suggested that U.S. government involvement would be helpful in establishing standards for technology development and interoperability to ensure that tools and technologies can be easily transferred from company to company along a supply chain in a reliable and secure way (Salit 2019). The National Institute of Standards and Technology already supports some activities developing synthetic biology standards (NIST 2019).

There was some discussion throughout the project about the potential for regulation or other legal instruments to compel specific actions or ensure adherence to specific standards. Currently, there are very few federal regulations for companies developing synthetic biology tools and capabilities (the horizontal bars in Figure 1), though some specific product categories (in the vertical bars) have been regulated for decades. Regulations that may apply, including export control and the Select Agent Regulations, are narrowly focused on the production of known pathogens. The only federal policy specific to the industry is the HHS Screening Framework Guidance (HHS 2010), a voluntary framework for DNA synthesis providers to screen customers and the DNA sequences that are ordered to help prevent the illicit use of sequences that may confer pathogenicity or toxicity. Most, though not all, participants in this project believed that the synthetic biology industry is best suited to voluntary frameworks (such as guidance) rather than regulatory oversight. Key reasons for this view included: many of the risks are not well defined and so would be difficult to articulate in a regulation (e.g., there are challenges for the HHS Guidance in defining which DNA sequences are of concern, even for the relatively well-established risk of pathogenicity); the slow pace of regulatory implementation is no

match for the rapidly changing industry and its potential risks; and regulations may be costly and limit innovative new technologies and approaches. Even so, many industry representatives believed that regulation is inevitable; that eventually, a high-profile incident involving synthetic biology or biotechnology will create a political need for additional oversight. In this case, some believed that the industry would need to show that it has rigorous practices already in place to avoid burdensome regulation. A more formal public-private partnership or venue for discussion could help ensure the appropriate level of oversight for the industry, both in anticipation of technology development and in response to unforeseen events.

In addition to specific ideas for potential next steps, this project showed that discussions between policy experts and industry representatives can help generate creative ideas about how the industry will look in the future and what types of policy frameworks should be developed over time. The workshop featured a discussion session on governance analogies that yielded implications that the U.S. government and others might consider on a longer time scale. The most common set of analogies was synthetic biology as information technology, artificial intelligence, and cyber capabilities (and vulnerabilities). In those fields, codes of conduct and other forms of self-governance have been dominant (though concerns abound that such oversight is inadequate). Workshop participants highlighted the opportunity and the need to understand governance challenges and lessons learned in those fields to apply to synthetic biology. The telecommunications industry, with its ongoing challenges with data management and complex manufacturing supply chains for cell phone production, may also provide useful lessons and precedents.

Other analogies included customer screening for the use of synthetic biology tools as similar to flying on a commercial airline, so perhaps governments should work to develop systems similar to TSA PreCheck for trusted users and spot checks for others. For some technologies, such as printers with anti-counterfeit measures that identify currency and will not print it, built-in safeguards prevent misuse of the technologies with no impact on (or even knowledge of) the user; DNA synthesis or other synthetic biology capabilities could pursue similar approaches. There are other products where society regulates, but has accepted some inherent risk, including alcoholic drinks, cars, and guns. Will society consider synthetic biology in similar terms? Will society consider synthetic biology capabilities to be more like consumer products with little necessary oversight? Only time will tell. Each of these technologies and products have policy frameworks that may have lessons relevant to the synthetic biology industry.

Conclusions

The U.S. government should establish an official, standing venue for discussion and interaction between U.S. policy makers and the synthetic biology industry to best harness the promise of synthetic biology, including its applications and its economic potential, while minimizing biosecurity risks. The synthetic biology industry is becoming an increasingly important part of the U.S. economy and will enable or improve a wide range of products in many different economic sectors. The companies that develop and apply synthetic biology tools and capabilities work within a complex industry ecosystem that is interconnected and interdependent, with a wide range of products and services, business models, and customer interactions. Biosecurity concerns arise as synthetic biology tools and capabilities become more widely available for use and more deeply integrated into products, services, and supply lines.

Our study, based on interviews and in-depth discussions with industry representatives, found that there are several aspects of today's synthetic biology industry that are most immediately relevant to

biosecurity. One key consideration is access by nefarious actors to synthetic biology tools and capabilities. We found that economic and business realities lead to a situation in which the most advanced capabilities are available primarily to well-paying customers (often, larger businesses) in long-term and collaborative arrangements that are not conducive to misuse of the technologies. For less powerful and more widely available technologies, including synthetic DNA and CRISPR-based genome editing tools, business practices such as customer screening can help minimize the potential for misuse. Other key considerations for biosecurity include the increasing digitization of synthetic biology tools and capabilities and the international nature of the industry. These factors may create vulnerabilities, particularly for data and intellectual property protection. These vulnerabilities are a challenge within each company, but may also constitute a national security risk as the industry's footprint in the U.S. economy continues to grow and the U.S., including DoD, comes to depend on synthetic biology products and services.

Companies that make up the synthetic biology industry currently use a wide range of business practices that may address these biosecurity risks. In project discussions and at the workshop, it was clear that there would be value in discussing different approaches, establishing best practices, and disseminating them throughout the industry. Areas where discussion of best practices would be helpful include customer screening, determination of potential risks for different types of technologies, and data and intellectual property protection. Although these discussions could be conducted among industry stakeholders without U.S. government involvement, support from the federal government could widen the discussions, help draw attention to the issue, and lend authority to the outcomes.

By establishing an official forum for multi-stakeholder discussions on synthetic biology and biosecurity, the U.S. government could gain insights into new capabilities and the trajectory of the industry, identify technologies of interest, and help establish best practices for biosecurity. Given the rapid growth of the synthetic biology industry and its complex and interconnected nature, regular meetings would be necessary to maintain awareness and discuss new issues as they arise. Such a forum could also help identify areas where new policy development might be appropriate. Indeed, successful implementation of biosecurity measures for the synthetic biology industry would require close coordination and co-development. Launching this effort should be an urgent priority so that it can be integrated into the fabric of the industry ecosystem as it grows.

References

Aharony N (2019) *Innovation in DIY Biology*. Johns Hopkins Center for Health Security. August 19. http://www.bifurcatedneedle.com/new-blog/2019/8/19/innovation-in-diy-biology

Arkin A, *et al.* (2018) KBase: The United States Department of Energy Systems Biology Knowledgebase. *Nature Biotechnology* 36:566–569. July 6. doi:10.1038/nbt.4163.

Barker JP, *et al.* (2018) *New Mandatory Submissions to CFIUS: Interim Regulations Under FIRRMA Take Effect November 10, 2018.* Arnold & Porter. https://www.arnoldporter.com/en/perspectives/publications/2018/10/new-mandatory-submissions-to-cfius

Bioeconomy Capital (2018) *Bioeconomy Dashboard: Economic Metrics*. Bioeconomy Capital. http://www.bioeconomycapital.com/bioeconomy-dashboard

BIS (Bureau of Industry and Security) (2017) *Chemical and Biological Controls.* U.S. Department of Commerce. https://www.bis.doc.gov/index.php/policy-guidance/product-guidance/chemical-and-biological-controls

Callaway E (2018) CRISPR plants now subject to tough GM laws in European Union. *Nature* 560:16. July 15. doi: 10.1038/d41586-018-05814-6

Canine W (2018) *The Synbio Stack, Part 1*. SynBioBeta. August 29. https://synbiobeta.com/the-synbio-stack-part-1/

Carlson R (2016) Estimating the biotech sector's contribution to the US economy. *Nature Biotechnology* 34:247–255. https://www.nature.com/articles/nbt.3491.

Carter SR and DiEuliis D (2019) Mapping the Synthetic Biology Industry: Implications for Biosecurity. *Health Security* 17(5). DOI: 10.1089/hs.2019.0078

Carter SR, Warner CM (2018). Trends in synthetic biology applications, tools, industry, and oversight and their security implications. *Health Security* 16(5):320-333. DOI: 10.1089/hs.2018.0067

Choulika A (2018) *The West is losing the gene editing race. It needs to catch up.* STAT. October 29. https://www.statnews.com/2018/10/29/west-is-losing-gene-editing-race/

Cohen J (2019) Fields of Dreams. *Science.* 365(6452):422-425. August 2. doi: 10.1126/science.365.6452.422

Cohen J and Desai N (2019) With its CRISPR revolution, China becomes a world leader in genome editing. *Science*. August 2. doi:10.1126/science.aay9689

Cumbers J (2019) The Bio-Belt: Growing the Future in Rural America. *Forbes.* July 15. https://www.forbes.com/sites/johncumbers/2019/07/15/the-bio-belt-growing-the-future-in-rural-america/#14f7a10f5461

Cyranoski D (2019a) The CRISPR-baby scandal: what's next for human gene-editing. *Nature* 566:440-442. February 26. doi: 10.1038/d41586-019-00673-1

Cyranoski D (2019b) China announces hefty fines for unauthorized collection of DNA. *Nature*. June 14. doi: 10.1038/d41586-019-01868-2

DiEuliis D (2018) Biotechnology for the Battlefield: In need of a strategy. *War on the Rocks.* November 27. https://warontherocks.com/2018/11/biotechnology-for-the-battlefield-in-need-of-a-strategy/

Export.gov (2019) *Consolidated Screening List*. U.S. Government. https://2016.export.gov/ecr/eg_main_023148.asp

Friedman J (2019a) *YC and Ginkgo Bioworks announce new partnership for synthetic biology startups.* YCombinator. September 16. https://blog.ycombinator.com/yc-and-ginkgo-bioworks-announce-new-partnership-for-synthetic-biology-startups/

Friedman J (2019b) *How Biotech Startup Funding Will Change in the Next 10 Years.* YCombinator. August 5. https://blog.ycombinator.com/how-biotech-startup-funding-will-change-in-the-next-10-years/

FSAP (Federal Select Agent Program) (2017) *Federal Select Agent Program.* U.S. Centers for Disease Control and Prevention and Department of Agriculture. https://www.selectagents.gov/

Gronvall G (2015) US Competitiveness in Synthetic Biology. *Health Security* 13(6):378-89. November-December. doi: 10.1089/hs.2015.0046.

Hancock T and Kuchler H (2019) Chinese VC spending on US biotech hit by security reviews. *Financial Times*. July 8. https://www.ft.com/content/6d647f7e-a13a-11e9-974c-ad1c6ab5efd1

HHS (Health and Human Services) (2010) *Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA*. U.S. Department of Health and Human Services. https://www.phe.gov/Preparedness/legal/guidance/syndna/Pages/default.aspx

HHS (2017) *Department of Health and Human Services Framework for Guiding Funding Decisions about Proposed Research Involving Enhanced Potential Pandemic Pathogens.* U.S. Department of Health and Human Services. https://www.phe.gov/s3/dualuse/Pages/p3co.aspx

Hoyt J (2017) *Top Accelerators and Incubators in China.* Globig. January 5. https://globig.co/blog/top-accelerators-and-incubators-in-china/

Hyde E (2019a) *Synthetic biology's Lego kit: Brought to you by Arzeda, TeselaGen, Twist Bioscience, and Labcyte.* SynBioBeta. August 31. https://synbiobeta.com/synthetic-biologys-lego-kit-brought-to-you-by-arzeda-teselagen-twist-bioscience-and-labcyte/

Hyde E (2019b) *Why China is primed to be the ultimate synbio market*. SynBioBeta. February 12. https://synbiobeta.com/why-china-is-primed-to-be-the-ultimate-synbio-market/

iGEM (International Genetically Engineered Machines) (2019) *Safety and Security Hub*. iGEM Foundation. https://2019.igem.org/Safety

JGI (Joint Genome Institute) (2019) *A DOE Office of Science National User Facility.* U.S. Department of Energy. https://jgi.doe.gov/

Kazmierczak M, Ritterson R, Gardner D, Casagrande R, Hanemann T, and Rosen DH (2019) *China's Biotechnology Development: The Role of US and Other Foreign Engagement.* Gryphon Scientific, LLC and Rhodium Group, LLC report to U.S.-China Economic and Security Review Commission. February. Available: https://www.uscc.gov/Research/china%E2%80%99s-biotechnology-development-role-us-and-other-foreign-engagement

Kirkpatrick J, *et al.* (2018) *Editing Biosecurity: Needs and Strategies for Governing Genome Editing*. https://editingbiosecurity.org

Klusty T and Weinmeyer R (2015) Supreme Court to Myriad Genetics: Synthetic DNA is Patentable but Isolated Genes Are Not. *AMA Journal of Ethics* 17(9):849-853. doi: 10.1001/journalofethics.2015.17.9.hlaw1-1509.

LeMieux J (2019) One-Stop-Shop Genome Editing Product Launched by Inscripta. *Genetic Engineering and Biotechnology News.* October 2. https://www.genengnews.com/insights/one-stop-shop-genome-editing-product-launched-by-inscripta/

Mauroni A (2018) Synthetic Biology: The Promise and Peril of a New Dual-Use Technology. *War on the Rocks*. August 10. https://warontherocks.com/2018/08/synthetic-biology-the-promise-and-peril-of-a-new-dual-use-technology/

Morton O (2005) Life, Reinvented. *Wired.* January 1. https://www.wired.com/2005/01/mit-3/

Murch R, So WK, Buchholz WG, Raman S, and Peccoud J (2018) Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy. *Front Bioeng Biotechnol* 6:39. April 5. doi: 10.3389/fbioe.2018.00039

Narayanan M (2019) Trump's trade war is hurting companies like mine — and the biotechnology industry. *STAT*. September 25. https://www.statnews.com/2019/09/25/trade-war-hurting-biotech-companies/

NASEM (National Academies of Science, Engineering, and Medicine) (2015) Industrialization of Biology: A Roadmap to Accelerate the Advanced Manufacturing of Chemicals. *National Academies Press,* Washington, DC.

NASEM (2016) Gene Drives on the Horizon: Advancing Science, Navigating Uncertainty, and Aligning Research with Public Values. *National Academies Press,* Washington, DC.

NASEM (2017) Preparing for Future Products of Biotechnology. *National Academies Press,* Washington, DC.

NASEM (2018) Biodefense in the Age of Synthetic Biology. *National Academies Press,* Washington, DC.

NCBI (National Center for Biotechnology Information) (2019) *GenBank Overview*. https://www.ncbi.nlm.nih.gov/genbank/

NIH (National Institutes of Health) (2019) *Dual Use Research of Concern*. NIH Office of Science Policy. https://osp.od.nih.gov/biotechnology/dual-use-research-of-concern/

NIST (U.S. National Institute of Standards and Technology) (2019) *NIST Living Measurement Systems Foundry.* NIST. https://www.nist.gov/programs-projects/nist-living-measurement-systems-foundry

Nouri B (2018) *A Realistic Perspective on post-Alice Software Patent Eligibility.* IPWatchdog. October 14. https://www.ipwatchdog.com/2018/10/14/realistic-perspective-post-alice-software-patent-eligibility/id=101977/

Rejeski D (2017) *Synthetic Biology in the United States: A Brief History of an Emerging Innovation System.* Environmental Law Institute. https://www.eli.org/technology-innovation-and-environment/innovating

Salit M (2019) *In synthetic biology, it's not only what you measure, but how you share it.* SynBioBeta. January 10. https://synbiobeta.com/in-synthetic-biology-its-not-only-what-you-measure-but-how-you-share-it/

Schmidt C, Costa KA, Limas M, and Cumbers J (2019) *Synthetic Biology Investment Report 2019 Q2.* SynBioBeta. July 19. https://synbiobeta.com/these-37-synthetic-biology-companies-raised-1-2b-this-quarter/

Zhang S (2018) A Biohacker Regrets Publicly Injecting Himself With CRISPR. *The Atlantic*. February 20. https://www.theatlantic.com/science/archive/2018/02/biohacking-stunts-crispr/553511/

Appendix A: Project Contributors

The following individuals contributed their perspectives and thoughtful comments through interviews, feedback on drafts of this report, and other discussions with the authors. Those with an * also participated in the workshop.

Matt Ball, Culture Biosciences*
Andy Baltus, Addgene*
Patrick Boyle, Ginkgo Bioworks*
Tim Brears, Evonetix
David Breslauer, Bolt Threads
Will Canine, OpenTrons
Rob Carlson, Bioeconomy Capital
Pete Carr, MIT Lincoln Labs
Rocco Casagrande, Gryphon Scientific*
Sunil Chandran, Amyris
Joel Cherry, Amyris
John Cumbers, SynBioBeta*
Tricia Delarosa, HHS*
Doug Densmore, Asimov and Boston Univ.
Kim de Mora, Addgene
James Diggans, Twist Biosciences*
Peter Emanuel, Army
Steve Evans, former Corteva*
Justin Farlow, Serotiny*
Mike Fero, TeselaGen*
Mark Fischer-Colbrie, LabCyte
Clem Fortman, EBRC*
Michal Galdzicki, Arzeda*
Jason Gammack, Inscripta
Fernando Garcia, Amyris*
Gigi Gronvall, Johns Hopkins University*
Dan Grushkin, GenSpace
John Hamer, DCVC
Karl Handelsman, Roche Venture
Ron Hann, DTRA*
Nathan Hillson, Berkeley National Lab*
Jiahao Huang, Nuclera
Austin Jelcick, former Vectorbuilder.com
Andy Kilianski, JPEO*
Jay Konieczka, EnEvolv
Mike Lee, Bolt Threads*
Peter Lee, Strateos
Alec Nielsen, Asimov
Dave O'Brochta, Foundation for NIH
Mike O'Keefe, LMI, support to DoD*
Kimberly Orr, Dept. of Commerce*
Megan Palmer, Stanford
Will Patrick, Culture Biosciences
Edward Perello, Arkurity*
Todd Peterson, Allen Institute
Dave Rejeski, Environmental Law Institute
Sarah Richardson, Microbyre*
Ryan Ritterson, Gryphon Scientific
Shahram Seyedin-Noor, Civilization Ventures*
Dave Shepherd, DHS*
Richard Stoner, Synthego*
Jessica Tucker, NIH Office of Science Policy*
Sean Ward, Synthace
Beth Vitalis, Inscripta
Ian Watson, White House OSTP*
Rachel West, Johns Hopkins University*
Kate Wildauer, former SynBioBeta
Ed You, FBI*

Appendix B: May 23–24, 2019 Workshop Agenda

SYNTHETIC BIOLOGY INDUSTRY PRACTICES AND OPPORTUNITIES (IPO) FOR BIOSECURITY
20 F Street Conference Center, Washington, DC

Thursday, May 23, 2019

8:30am	Registration and breakfast
9:00	Opening remarks and introductions around the table Speakers: Sarah Carter, Diane DiEuliis
9:30	Industry landscape and emerging themes Notes from industry interviews: Sarah Carter Discussion
10:30	BREAK
10:45	What Kinds of Misuse/Risks are we Worried About? (5 min) Notes from industry interviews: Diane DiEuliis (10 min) NASEM report: Gigi Gronvall, Johns Hopkins Center for Health Security (10 min) Laboratory automation/outsourcing: Rocco Casagrande, Gryphon Scientific (10 min) Biosecurity and Genome Editing: Edward Perello, Arkurity Discussion
12:15pm	LUNCH
1:15	Customer Screening (5 minutes) Framework overview: Sarah Carter (10 min) Customer screening procedures: Andy Baltus, Addgene (10 min) Customer screening procedures: James Diggans, Twist Discussion
2:30	BREAK
2:45	Navigating Vulnerabilities and Understanding Responsibilities (10 min) Cyberbiosecurity: Diane DiEuliis (10 min) Import/export rules: Kimberly Orr, Dept of Commerce (10 min) Law Enforcement and National Security: Ed You, FBI Discussion
4:00	Day 1 Closing Remarks and Adjourn
6:00	Dinner

Friday, May 24, 2019

8:15am	Breakfast
8:45	Prior day Recap Sarah Carter, Diane DiEuliis
9:15	Analogies for understanding the industry's future, due diligence, and policy options (5-10 minutes) Notes from interviews: Sarah Carter, Diane DiEuliis Discussion
10:30	BREAK
10:45	How can the U.S. Government Assist Companies with Due Diligence? (10 min) HHS Screening Framework Guidance: Tricia Delarosa, HHS (10 min) Notes from industry interviews: Sarah Carter Discussion
12:00pm	LUNCH
1:00	Summary of discussion and final points of consensus and/or divergence Sarah Carter, Diane DiEuliis
2:00	Adjourn

Appendix C: Acknowledgements

We would like to thank the Defense Threat Reduction Agency (DTRA) for funding this project through its Project for Advanced Systems and Concepts for Countering WMDs (PASCC), which is now housed within the Strategic Trends Office at DTRA. Dr. DiEuliis was also supported by the Center for the Study of Weapons of Mass Destruction at National Defense University, including Elizabeth Wright and Nick Winstead.

This project would not have been possible without the dozens of people within the synthetic biology industry, the U.S. government, and other organizations who took the time to answer our emails, speak with us, and come to our workshop. Many of these individuals are listed in Appendix B as project contributors. We would also like to specifically thank John Cumbers for making it possible for us to discuss and present this project at SynBioBeta, and Rachel West for her help and support at the workshop.

Appendix D: About the Authors

Sarah R. Carter is the Principal at Science Policy Consulting LLC where she focuses on societal and policy implications of emerging biotechnologies, including issues of biosecurity, biosafety, environmental impacts, and responsible innovation. Previously, she spent five years in the Policy Center of the J. Craig Venter Institute, where she led projects on the accelerating pace of synthetic biology and the challenges it creates for policy makers, including a project on the biosecurity implications of DNA synthesis and the hurdles faced by industry in addressing those concerns. In 2009–2010, Dr. Carter worked at the White House Office of Science and Technology Policy (OSTP) where she focused on issues relating to climate change and sustainability. She is also a former AAAS Science & Technology Policy Fellow and a former Mirzayan Fellow of the National Academies. She earned her Ph.D. in Neuroscience from the University of California, San Francisco and her bachelor's degree in Biology from Duke University. Email: carter@sciencepolicyconsulting.com.

Diane DiEuliis is a Senior Research fellow at National Defense University. Her research areas focus on emerging biological technologies, biodefense, and preparedness for biothreats; she has specifically studied issues related to synthetic biology, the US bioeconomy, and behavioral, cognitive, and social science as it relates to important aspects of biodefense. Prior to joining NDU, Dr. DiEuliis was the Deputy Director for Policy, in the Office of the Assistant Secretary for Preparedness and Response (ASPR), U.S. Department of Health and Human Services. While there, she coordinated policy in support of domestic and international health emergencies. Prior to that, Dr. DiEuliis served as the Assistant Director for Life Sciences and Behavioral and Social Sciences in the Office of Science and Technology Policy (OSTP) in the Executive Office of the President, where she was she was responsible for developing policy in areas such as biosecurity, research funding and administration, social and behavioral science, scientific collections, bioethics, and STEM education.