Testimony of Dr. Charles Clancy

Chief Technology Officer, MITRE

before the House Select Committee on Strategic Competition between the United States and the Chinese Communist Party,
Hearing on Growing Stakes: The Bioeconomy and American National Security

7 March 2024

Chairman Gallagher, Ranking Member Krishnamoorthi, and Committee Members:

My name is Charles Clancy, and I am a Senior Vice President and Chief Technology Officer at MITRE where I lead science, technology, and engineering for the company. MITRE is a non-profit, non-partisan research institution that operates Federally Funded Research and Development Centers on behalf of the U.S. Government.

Prior to joining MITRE, I spent nine years as a member of the faculty at Virginia Tech where I held the Bradley Distinguished Professorship of Cybersecurity in the Department of Electrical and Computer Engineering, and served as executive director of what is now the Virginia Tech National Security Institute. I started my career at the National Security Agency leading advanced research and development programs.

It is my pleasure to address this committee.

Introduction

The scope of this hearing is significant, as the bioeconomy broadly includes biotechnology, biomedicine, bioagriculture, biomanufacturing, and biosecurity. Scientific research into quantum mechanics 100 years ago led to today's semiconductors and booming technology economy, and we're at the same point in unlocking our understanding of cellular biology which will fundamentally transform our society again over the next century.

A common observation across most technology domains, over the past ten years the U.S. led the world in biotech research, development, and commercialization, but outsourced much of biomanufacturing and a myriad of related bioservices to places like China. As we reexamine our globalized trade relationships and supply chains, we realize that this outsourcing has created

significant risk. Additionally, not content to simply manufacture, China has invested heavily in R&D and has caught up to the U.S. in biotech, with major ongoing state-directed investments positioning them to take the lead.

Security is a major concern. One way China likes to catch up is to cheat – stealing intellectual property – and the U.S. research security apparatus needs to be updated to reflect risks across all critical emerging technologies. Another aspect of security is the cyber risk to our bioindustrial systems. The bioeconomy is not currently a designated critical infrastructure sector on its own[1], nor is it identified as a critical manufacturing sector.[2] As a result, key parts of are not able to benefit from federal cybersecurity resources. Lastly, since the global pandemic, the implications of biosecurity are increasingly top of mind, with ample opportunities to improve.

Two years ago, MITRE published a set of recommendations for congressional action to maintain U.S. leadership in advanced biotechnology[3], and they are included as an attachment to my written testimony. In the interest of time, I will focus on a subset of the recommendations in my opening remarks focused on how we can secure the bioeconomy and steps the US can take to mitigate increasing risks.

Decentralization

In the telecommunications area, the U.S.'s technology strategy to compete with China focuses on decentralization: the open radio access network, or "O-RAN," approach takes heretofore monolithic cell tower technology and breaks it into functional building blocks. By standardizing the interfaces we can diversify our supply chain, enable new market entrants, and take advantage of networked innovation. This same approach has applicability across many technology areas[4], including biology.

At MITRE we are leading an initiative to build a *BioNet*. With the trend to virtualize and automate bio-chemical laboratories, often called "cloud labs" or "self-driving labs," a BioNet is a software and programming layer that sits on top focused on biologic research, development, and production[5]. With standardized interfaces and data formats we can achieve interoperability at scale

---

[1] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
[2] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/critical-manufacturing-sector
[3] https://www.mitre.org/sites/default/files/2022-05/pr-22-00151-01-maintaining-us-leadership-in-advanced-biotechnology-growing-the-bioeconomy.pdf
[4] https://www.mitre.org/sites/default/files/2023-09/PR-23-2889-Decentralized-Innovation.pdf
[5] https://www.linkedin.com/pulse/bionet-update-building-coalition-steward-net-marc-salit-rybze/

to advance the bioeconomy. Existing federal investments in biomanufacturing, such as DOE's Agile Biofoundry program and DOD's BioMADE program could be further resourced to build the core for a BioNet.

Cybersecurity

While automation and internetworking enables entirely new innovation pathways for biology, it amplifies existing and creates new cybersecurity risks. Currently biology is not represented directly among our established critical infrastructure sectors, though aspects of it show up in agriculture and healthcare. At a minimum, biomanufacturing should be added to the officially designated critical manufacturing sectors, and that could provide a federal touchpoint for the relatively new Bioeconomy Information Sharing and Analysis Center, the Bio-ISAC[6].

However, in the biology domain, security risks are certainly broader than bioindustrial cybersecurity. A public-private partnership should be launched that is able to provide more operational support to the cyber-bio-security continuum. This partnership could also support a wide range of biosecurity and biosafety activities, particularly as decentralization and a BioNet provide common infrastructure and standards.

Research Security

As we make investments in R&D to support growing the bioeconomy, a final area of concern is research security. Today research security varies considerably across universities, startups, and companies. This creates a considerable risk that China fast-follows our R&D by stealing the intellectual property out from under us. And while today we are discussing this as it relates to biotechnology, the same issue applies to all areas of critical emerging technologies, from quantum to artificial intelligence.

For example, at universities executing restricted research, such as projects that involve controlled unclassified information or export-controlled technologies, work is limited to U.S. citizens and permanent residents, and information technology systems employed must adhere to certain cybersecurity standards[7]. However, the majority of research conducted in critical emerging technologies is designated fundamental research and exempted from these requirements.

---

[6] https://www.isac.bio/

[7] https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

National Security Presidential Memorandum (NSPM) 33[8] mandates the establishment of an intermediate category of research security for federally funded work in designated critical emerging technology areas[9], regardless of the funding instrument and sponsoring agency. While open to foreign national participation, there are new requirements to report information on foreign research participants. However, it remains unclear how this information will be used at scale, beyond simply the deterrent value of reporting. The Department of Justice should establish a clearinghouse to work with funding agencies, universities, and laboratories and perform personnel screening based on these disclosures, such as a National Agency Check, like suitability determinations performed for federal employees and contractors. This same clearinghouse could help enhance current screening processes for student (F-1), temporary worker (H-1B), and exchange visitor (J-1) visas.

Additionally, enhanced but achievable cybersecurity protections are essential, and are also part of the NSPM-33 docket. At a minimum, universities and research organizations receiving federal funding for critical emerging technology research should be required to implement network-based threat monitoring, zero-trust endpoints, data loss detection and prevention tools, and multifactor authentication. These are consistent with the requirements of NSPM-33, but many are still waiting on the final rules expected later this year to understand the implications and implementation complexities. Regardless, implementing these new requirements will be a significant burden to some universities, and science funding agencies, such as the National Science Foundation (NSF), could provide capacity building grants to help organizations with up-front expenses. Additionally, the NSF should move expeditiously to establish the proposed Research Security Information Sharing and Analysis Center (RS-ISAC)[10] to help provide a focal point for threat intelligence and information sharing.

Conclusion

In closing, we're sitting at an inflection point where biology offers huge potential to fundamentally transform society for the better. But we're in a globally competitive environment and we need to align policies and resources, and plug security holes, to be successful in the long term.

---

[8] https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf
[9] https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf
[10] https://new.nsf.gov/funding/opportunities/research-security-integrity-information-sharing/nsf23-613/solicitation

MAINTAINING US LEADERSHIP IN ADVANCED BIOTECHNOLOGY & GROWING THE BIOECONOMY

By Dr. John Dileo, Dr. Kunal Rambhia, Dr. Matt Downs, Dr. Janelle Rowell, and Caroline Kennedy

9 Recommendations for Congressional Action to Support the Growth and Security of the US Bioeconomy

1. **Build the necessary infrastructure to accelerate biotechnology innovation.** Develop a network of interoperable, highly automated, and interconnected research facilities at the local, regional, and national levels (a BioNet) that will enable rapid execution of projects through coordinated efforts, produce a fully developed biology-as-technology ecosystem, and enhance equity by making cutting edge technologies for engineering biology available to researchers that would otherwise not have such access.

2. **Support research and development investments to provide the foundation for the future US bioeconomy.** The bioeconomy will be driven by the commercialization of fundamental discoveries in biotechnology. Accelerating the pace of breakthrough discoveries will require strong and strategically coordinated R&D initiatives over the next few years across the basic-applied-advanced spectrum. Relatedly, the US will need to expand its biomanufacturing capacity to ensure future national security and economic prosperity from these R&D investments.

3. **Establish programs that develop a highly trained biotechnology workforce.** As the bioeconomy expands, the US biotechnology industry will require personnel with a broad spectrum of biotechnology knowledge and interdisciplinary skills. Developing the workforce will require new policies and programs that expand biotechnology education/training at all levels; enhance access to biotechnology and science, technology, engineering, and mathematical (STEM) education in underserved populations; provide for upskilling and retaining of workers; and encourage cross-disciplinary training.

4. **Facilitate trusted information sharing between public and private stakeholders in the bioeconomic ecosystem.** Explore development of an independent public-private partnership (PPP) to enable data sharing and open discussions of bioeconomic issues of concern while protecting government and industry partners' privacy and interests. An approach similar to the MITRE-managed Aviation Safety Information Analysis and Sharing (ASIAS) public-private partnership would be beneficial, as it allows rapid dissemination of threat information across the bioeconomy and sharing of best practices while protecting government and industry partners' privacy and interests.

5. **Set appropriate standards and regulations for biotechnology activities.** Technical standards should pair with regulations to reduce barriers, increase speed and predictability, and reduce costs, while protecting human and environmental health. A coalition inclusive of academia, industry, and government should be established to collaboratively draft technical standards and regulations. The development of interoperability standards, benchmarked production standards, and clear and well understood regulatory frameworks will contribute to the acceleration of technical discovery by primary researchers as well as reduce uncertainty for producers, allowing for more rapid commercialization of products.

6. **Address biosafety and biosecurity concerns associated with advanced biotechnology.** The US Government (USG) should work with academia, industry, and international partners to incorporate biosafety as an integral part of the BioNet and develop and disseminate best practices. Such efforts will ensure the responsible use of advanced biotechnology and reduce the likelihood of unintended adverse consequences.

7. **Assess biotechnology as critical infrastructure.** As biomanufacturing will soon become a common and important aspect to US national security and economic prosperity, the infrastructure associated with this sector must be protected from physical and cyber threats. Therefore, biomanufacturing should be included within the Department of Homeland Security's Critical Manufacturing Sector supporting Presidential Policy Directive 21, and "Supply Active Pharmaceutical Ingredients and Biological Precursors" should be designated as a National Critical Function. Doing so refines and clarifies roles and expectations for all entities with a role in protecting biomanufacturing assets.

8. **Identify threats to the bioeconomy.** USG should conduct a comprehensive risk assessment of current, future, and emerging threats to the bioeconomy and develop a mitigation plan. This would result in a dataset that captures the totality of biotechnology and biomanufacturing commodity and services flow domestically to and from US ports of entry. This dataset, combined with intelligence information on foreign threats and intentions, will identify key activities, infrastructure, and knowledge that must be protected.

9. **Take initial actions and plan for long-term efforts to mitigate threats to the bioeconomy.** Based on the risk assessment, a plan of action for addressing key vulnerabilities should be developed and maintained. In the near term, efforts should be undertaken to augment existing processes for protecting US intellectual property (IP) such as CFIUS reviews; enhance cybersecurity practices across the biotechnology enterprise by establishing a testbed capability for evaluating cyber vulnerabilities in bioeconomy associated equipment, software, databases, and information technology infrastructure; and prevent intangible technology transfer of key biological products, processes, and datasets. Additional specific actions will depend on the result of the threat assessment.

MITRE is a non-profit public interest organization that operates six federally funded research and development centers (FFRDCs) in support of USG missions. This plan was developed by MITRE experts in biosecurity, with inputs from experts in establishing public-private partnerships[1], cyber security[2,3], performing threat assessments[4], supply chain risk management[5,6], and data analytics.

Maintaining US Leadership in Advanced Biotechnology & Growing the Bioeconomy

In 2012, the Obama White House issued the National Bioeconomy Blueprint, which defined strategic objectives for the US Government (USG) to achieve the potential of a US bioeconomy that can "enable new discoveries through basic research, foster economic growth, and create new jobs[7]." In the past 10 years, the pace of innovation within and industrialization of the bioeconomy has increased substantially[8]. Driven by market opportunities and global crises (such as the COVID-19 pandemic), technologies that enable the use of biology to address a broad range of industrial applications have accelerated from basic academic research to full scale industrial manufacturing[9]. **The continued development and industrialization of the bioeconomy will have tremendous impacts in areas such as human health, manufacturing, the environment, and agriculture.** The potential societal benefits of a robust bioeconomy include increased energy independence, improved human health, and new ways to address environmental and climate challenges, to name a few. With these advances come global competition and new biological threats that will necessitate intentional policy and investment to secure the bioeconomy and protect US geopolitical interests.

As the vast majority of advancements that enable the growth of the bioeconomy were developed in the US, we have enjoyed a leading position in the development of commercial applications of biotechnology. From early efforts to develop genetically modified bacteria that degrade oil for use in environmental remediation applications to current efforts described below, the US has been (and remains) the recognized global leader in biotechnology[10]. However, the rest of the world has not failed to notice the potential of biotechnology to provide an economic boost and develop solutions to country-specific problems, such as new crops to feed their growing populations, new medicines to treat old illnesses, as well as solutions to problems associated with aging populations, mitigating effects of climate change, and finding better ways to use their abundant natural resources sustainably.

Both allies and near peer competitors are using industrial policy, economic incentives, and large national investments to execute national roadmaps designed to develop intrinsic biotechnology industries that equal (or surpass) the US. India's expressed desire to capitalize on its large educated populous to bring in foreign investment[11] and Egypt's National Strategy for Genetic Engineering and Biotechnology[12] are just two of many examples of such government initiatives. In addition to national-level efforts, the highly interconnected nature of the scientific community and the rapid global dissemination of biotechnical knowledge and technologies are aiding catch-up efforts by allowing individuals, novices, small groups, and nations to rapidly become involved in biotechnology and perform advanced research resulting in the potential for "Biotechnology Breakout Programs."

Competitors are rapidly catching up to the US with varying levels of success. The most well know example of rapid and significant biotechnology investment is occurring in China under the Made in China 2025 Strategy[13] and other efforts. According to the 2019 report on the US-China Economic and Security Review Commission[14], China's biotechnology industry has rapidly grown but remains only 1/10 the size of the US industry. However, China is rapidly closing this gap through top-down government direction, a national talent recruitment strategy, and high R&D spending. Over the past 6 years, China's investment in the biotechnology industry has surpassed $500B per year. China's significant control over the bioeconomic supply chain,

manufacturing capacity, and ability to spend large sums on R&D is giving China significant and growing influence in this industry, potentially threatening critical US manufacturing capabilities.

In order to respond to this increase in competition, to ensure that the US maintains its leadership in biotechnology, to prevent leapfrogging, and to develop biotechnology-enabled capabilities, a robust biotech industrial base and a growing bioeconomy are required. While US capabilities are impressive, the full potential of biotechnology to impact areas such as human health, manufacturing, the environment, and agriculture have not been fully realized. An expanding bioeconomy will not only drive economic growth by providing technologies, products, and services, but also contribute to national security by reducing adversary control over supply chains, key intermediaries, and technologies, allowing for more sustainable and effective use of natural resources and positioning the US to set the terms of the debate surrounding best practices for performing biotechnology research safely and ethically.

Given all these indicators, a government-wide strategic coordinating body tasked with safeguarding and realizing the potential of the US bioeconomy should be established. To be successful, this coordinating body should be presided over by senior White House leadership, with representation from scientific, economic, regulatory, and security agencies. It should be responsible for relevant foresight activities and be informed by input from a diverse range of relevant external stakeholders. The coordinating body should develop, adopt, and then regularly update a living strategy with goals for sustaining and growing the US bioeconomy. This strategy should be informed by an ongoing, formal horizon-scanning process within each of the relevant science agencies, as well as by input from industry, nongovernmental organizations, and academia. Additionally, through this strategy, the coordinating body should identify and raise awareness of means through which the US Government can advance the bioeconomy, including such existing means as government procurement of bio-based products. MITRE recommends this coordinating body undertake the actions outlined below, at a minimum.

Build the necessary infrastructure to accelerate biotechnology innovation.

Maximizing the productivity of the US biotech enterprise will require expanding access to the advanced tools and capabilities referenced above as widely as possible across academia, industry, and government. A plan for building a network of interoperable, highly automated, and interconnected research facilities at the local, regional, and national levels (a BioNet) should be developed. Under internal funding, MITRE recently kicked off a Biotechnology Moonshot effort with the goal of creating a model BioNet focused on national security applications. This effort is focused on utilizing systems engineering concepts to create a web of researchers, suppliers, vendors, and producers in which materials, procedures, requirements, and data are seamlessly shared among partners to allow for the agile development of research programs, development of products, and scale-up and production. This effort could serve as an exemplar for how to establish a distributed and networked bioeconomy that can be scaled. Efforts to build networks of cloud-based labs and initiatives to expand access to pilot scale production capabilities (e.g., Department of Defense sponsored BioMADE MII) are currently ongoing and could serve as the backbone of a BioNet.

The networked biological research and biofoundries making up the BioNet should be encouraged to pool resources, knowledge, and expertise to learn from successes and failures. This can be achieved through the development of data and knowledge repositories. Large scale data repositories on biological systems can drive the generation of novel biological research hypotheses. Applying advanced artificial intelligence

(AI) methods to data mine the results, both successes and failures, will generate sharable knowledge across the partnership, and this is currently being done on individual scales within genomics, proteomics, and metabolomics. However, a uniform data repository will allow for the discovery of novel information and development of future hypotheses. Funding should be dedicated for developing and augmenting currently available high-performance computing clusters to support these efforts.

The development of a BioNet-enabled research enterprise will support the execution of cutting edge research projects through coordinated efforts, produce a fully developed biology-as-technology ecosystem, and enhance equity by making cutting edge technologies for engineering biology available to researchers that would otherwise not have such access.

Support R&D investments to provide the foundation for the future US bioeconomy.

Currently, the US is the world leader in advanced biotechnology, and maintaining this leadership will require continued investment in fundamental and cross-cutting science and technology related to the design, fabrication, and testing of engineered biological systems. The development of commercially viable biotechnology products and services will require investment in fundamental and cross-cutting science and technology efforts that develop fundamental tools and technologies that enable biotechnology research. This can include, but is not limited to, prioritizing activities that:

- Develop AI/design tools; computational tools and environments for performing biosystems design, modeling, and simulation; and experimental processes and equipment for implementing designed or modified biological parts, components, and systems.
- Conduct fundamental and applied research related to advanced biomanufacturing; DNA synthesis, sequencing, and engineering; biomolecular pathway discovery and engineering; host utilization, characterization, and engineering; data science; and high-throughput screening and optimization.
- Enable and accelerate the design, build, and test of biological components and systems.
- Enable high-throughput process optimization (R&D to test and evaluation).
- Develop standardized discovery workflows.

The sustained technology push from researchers will drive the development of concepts for commercial products, but taking breakthrough discoveries to marketed products will require translational research funding to bridge the gap between lab to market. Current funding mechanisms should be reviewed and improved to better support the transition from lab to production and adoption. These funding mechanisms should include both those internal to government organizations as well as those available for academia and industry. In addition to financial support, these mechanisms should provide access to guidance and resources for navigating necessary regulatory approval and adoption. Transitional funding should be closely tied with key strategic government needs, with awardees working closely with the government sponsors to ensure ease of transition and fielding of the product.

Like any rapidly growing and nascent industry, it is likely that industry will inevitably focus on activities that are most profitable and not necessarily aligned with USG national security needs. USG should work to incentivize industry to expand biomanufacturing capacity for USG national security needs and should use national security mission requirements to pull innovation forward. USG should further leverage technological advances that emerge from a robust bioeconomy to support critical national security missions, including pandemic prevention and preparedness.

Investing in foundational biological engineering technologies will accelerate the pace of biomedical discovery and will allow for the development of breakthrough bio-capabilities. This ecosystem of biotech innovation will foster the continued development of additional capabilities in a virtuous cycle.

Establish programs that develop a highly trained biotechnology workforce.

As the bioeconomy expands, the US biotechnology industry will require personnel with a broad spectrum of biotechnology knowledge and skills ranging from technicians with basic understanding of biological concepts to experts with doctoral degrees and years of experience in applied research. Given the growing overlap between biotechnology, information technology, and engineering, this workforce will include both positions staffed by experts in biological principles (e.g., molecular biologists, geneticists, computational biologists, systems biologists, microbiologists, biochemists) with secondary understanding of engineering principles, and positions where expertise lies in a non-biologically related STEM field (e.g., engineering, materials science, chemistry, data science, cybersecurity) with a working understanding of biological principles. As biotechnology as a technology penetrates a larger portion of the economy, workers in ancillary industries may need some upskilling to gain an understanding of a variety of basic biotechnology principles in order to effectively take advantage of the opportunities created. Developing the workforce will require the development of new policies, training, and outreach programs focused on expanding biotechnology education/training such as those that:

- Enhance biotech education and training at all levels (K–12 through graduate).
- Enhance biotechnology and STEM education in historically underserved populations.
- Encourage cross-disciplinary training in biotechnology and engineering.
- Provide training in biological systems engineering and biological design.
- Provide training, retraining, and continuing education in laboratory skills.
- Establish/enhance university and advanced graduate degree programs in core and non-core biotechnology fields.
- Provide vocational training, co-operative programs, internships/apprenticeships, or post-doctoral training opportunities.

USG support of efforts that increase biotechnology literacy across the workforce will result in an increased pool of qualified workers to support the growing bioeconomy.

Facilitate trusted information sharing between public and private stakeholders in the bioeconomy ecosystem.

The BioNet is by nature a web of academic, industry, and government organizations with the common goal of maximizing the potential of biotechnology. The effective protection of this web will be greatly enhanced by the establishment of an independent public-private partnership (PPP) focused on sharing threat information across the industry. A model of such a partnership is the Federal Aviation Administration's Aviation Safety Information Analysis and Sharing (ASIAS) system. In this system "airline safety data is safeguarded by The MITRE Corporation, in a de-identified manner to foster broad participation and engagement. ASIAS fuses various aviation data sources to proactively identify safety trends and to assess the impact of changes in the aviation operating environment[15]." In using an FFRDC, the PPP would have a firewall between government and industry, albeit an appropriately porous one that allows data in and data out with anonymization in between. Select activities of such a PPP could include conducting a Policy Review

to ensure deconfliction and alignment of policy, regulations, and programs; performing analysis of collected data to identify threats and risks; creating a group within the PPP composed of USG personnel with access to relevant classified information to conduct threat assessments, sanitize findings, and distribute to non-cleared PPP partners to inform their security postures and policies; and conducting bioeconomic security R&D, as advised by a body such as the Critical Manufacturing Government Coordinating Council (GCC) and Sector Coordinating Council (SCC), post inclusion of Biomanufacturing as a Critical Manufacturing Sector component. Applying an ASIAS-like model to the biotechnology sector would enable the sharing of best practices for security and dissemination of threat information, and enable open discussions of bioeconomic issues of concern while protecting government and industry partners' privacy and interests.

Set appropriate standards and regulations for biotechnology activities.

A fully operational BioNet will require technical standards and regulations that ensure interoperability, reduce barriers, increase speed and predictability, and reduce costs while protecting human and environmental health. The standards and regulations need to be clear to researchers and manufacturers to promote reproduceable results and to not hinder progress or US competitiveness in this rapidly growing field of the international bioeconomy.

A collaborative approach should be taken to establish standards through a coalition that spans across academia, industry, and government organizations. A coalition focused on these topics is being developed under the MITRE BioNet Initiative and could be an initial forum for undertaking the activities described here. Key areas of focus should include establishing standards for physical materials, specifying biological designs, exchanging experimental protocols, describing biological systems with data, storing data, defining the interfaces between functional components of the BioNet, and ensuring security and privacy, as well as developing standardized verification and validation metrics. The coalition can leverage ongoing standard setting, regulatory, and metrology activities within the National Institute of Standards and Technology (NIST), National Institutes of Health's National Center for Biotechnology Information (NIH NCBI), and DoD organizations, as well as current standards for materials, devices, and organisms, with an action to explore future or "could be" research questions, practices, and results that would require standards and regulations being revised.

Interoperability standards, benchmarked production standards for networked biofoundries and research labs, and clear and well understood regulatory frameworks will contribute to the acceleration of technical discovery by primary researchers as well as reduce uncertainty for producers, allowing for more rapid commercialization of products.

Address biosafety and biosecurity concerns associated with advanced biotechnology.

As access to advanced biological methods becomes more widely available, as advanced biotech penetrates industrial processes, and as bio-enabled products reach the commercial market, the potential for accidental or deliberate misuse of these technologies or unforeseen impacts on human health or the environment must be avoided and mitigated. Biosafety should be an integral part of the BioNet, and USG should encourage the development of global best practices that ensure the responsible use of advanced biotechnological products through engagements with academia, industry, and

international partners. Priority should be given to scientific, technical, and policy efforts that:

- Augment existing national and international efforts related to biosecurity.
- Develop tools and methods for assessing potential risks that engineered biological systems could pose to human health (e.g., engineered infectious pathogens with increased transmissibility, virulence, or ability to evade countermeasures) or the environment.
- Enhance the oversight of the production of genes or gene fragments that could be misused (e.g., California Assembly Bill-70 Gene Synthesis Providers would have, if enacted, required gene synthesis providers and manufacturers of gene synthesis equipment to abide by customer and sequence screening protocols[16]) to cause harm or economic disruption, without stifling the economic opportunities and growth potential of the bioeconomy.
- Establish national and/or international norms for the use of advanced biotechnology.
- Identify opportunities for USG to engage/establish formal parternerships with participant nations on mutually beneficial research priorities that can be achieved via biotechnology.
- Preserve strategic and technological advantage over competitors and adversaries who would use biotechnology for purposes inconsistent with US values.
- Collaborate with partner nations to advance the emerging field of biotechnology in safe and responsible ways consistent with the legal and ethical "norms" expected by democratic countries.
- Strengthen the ecosystem of US/international biotechnology engagements/projects/efforts.

Taken together, these and similar steps will ensure the responsible use of advanced biotechnology and reduce the likelihood of unintended adverse consequences. Continued engagement in this field will allow the US to set the tone for this debate, drive international consensus on the best practices and policies for safely and ethically engineering biology, and set limits on the acceptable use of the products of engineered biology. These efforts will result in the creation of a biotechnology ecosystem of national and international alliances that enable the advancemnt of biotechnology while ensuring it is used responsibly.

Assess biotechnology as critical infrastructure.

As biomanufacturing becomes ever more common and important to US national security, the infrastructure associated with this sector must be protected from physical and cyber threats. Therefore, biomanufacturing should be included as the fifth manufacturing industry included in the Critical Manufacturing Sector[17] under the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and/or "Supply APIs and Biological Precursors" should be designated as a National Critical Function[18]. Doing so would initiate a cascade of established means through which to secure the biomanufacturing and biotechnology sectors. That cascade may include incorporating a biomanufacturing industry-specific section into the Critical Manufacturing Sector-specific plan and including subject matter experts with biomanufacturing expertise on the Critical Manufacturing GCC and SCC to share information and identify R&D opportunities[19]. It may also include leveraging the National Risk Management Center to "identify, analyze, prioritize, and manage the most significant risks" to supplying APIs and biological precursors. By incorporating biomanufacturing and biotechnology into existing critical infrastructure mechanisms like Critical Infrastructure Sectors and National Critical Functions, whole-of-government

resources would have a clear avenue for application, and previously defined roadmaps for engagement with industry could also be leveraged.

Identify threats to the bioeconomy.

As the bioeconomy becomes an increasingly larger segment of the economy and more important to national security, it is imperative that the US protect the infrastructure, knowledge, and data associated with this sector. As competitor nations seek to outpace the US in biotechnology activities, direct attacks on bio infrastructure such as the recent Tardigrade malware attack on biomanufacturing organizations[20], theft of intellectual property by aggressive near peer competitors[21], and direct or intangible tech transfer to non-US companies via mergers, acquisitions, capital investment, and research collaborations[22] are increasingly likely.

The first step in planning for such eventualities should be to conduct a comprehensive risk assessment of current, future, and emerging threats to the bioeconomy and to develop a mitigation plan. Such a risk assessment would identify parts of the bioeconomy and its supply chain that are critical to national security and competitiveness and make recommendations for ensuring those are protected. This would also involve modeling of the current biotechnology and biomanufacturing supply chains to identify regions, companies, and services critical to the resilience of the supply chains. This would require developing a dataset that captures the totality of biotechnology and biomanufacturing commodity and service flows domestically and to and from US ports of entry. To understand the vulnerabilities in the biotechnology and biomanufacturing sector, these datasets can be used to map commodity and service flows and analyze key supply chains related to items such as active pharmaceutical ingredients (APIs), key intermediates related to national security, and biomass required for biomanufacturing, among others. Combined with intelligence information on foreign threats and intentions, this assessment would identify key activities, infrastructure, and knowledge that must be protected. One such analysis that can be built on is the recently published MITRE 10-Point Action Plan: Sustaining a Biopharma Industrial Base for a More Secure Nation, which makes policy and programmatic recommendations to ensure the US has a strong and sustainable biopharma industrial base[23].

Take initial actions and plan for long-term efforts to mitigate threats to the bioeconomy.

Based on the threat assessment, a plan of action for addressing key vulnerabilities should be developed. While the specific actions will depend on the result of the threat assessment, some initial actions that could be immediately undertaken include augmenting existing processes for protecting US intellectual property (IP); enhancing cybersecurity practices across the biotechnology enterprise; and preventing intangible technology transfer of key biological products, processes, and datasets.

To better understand the implication of proposed mergers and acquisitions and prevent the transfer of key or national security critical IP, USG should leverage the contracting mechanisms available to the members of the interagency Committee on Foreign Investments in the US (CFIUS) to expand the cadre of technical subject matter experts (SMEs) available to participate in reviews on an as-needed basis. Though the makeup of CFIUS is varied, and includes individuals from numerous technical backgrounds, the pace of biotechnological advancement is such that additional subject matter expertise may, at times, be needed to make fully informed transaction determinations relevant to emerging biotechnologies. CFIUS could bring on cleared SMEs for short-term adjudications by tapping existing contracts that

interagency members (e.g., Department of Treasury, DoD, Office of Science and Technology Policy) have with academia, industry, or FFRDCs.

Cleared SMEs brought on to support CFIUS could leverage processes and programs that semi-automate, and thereby increase efficiency of, foreign investment investigations. Over the past several years, MITRE has developed expertise in the analysis of non-traditional data (e.g., economic data, open source information, business intelligence), which has been utilized to perform analyses of global supply chains and corporate relationships in the biotechnology sector that could be modified to conduct foreign investment vetting quickly and provide confidence ratings associated with the outputs. Such programs could reduce burden on CFIUS staff, increase the speed with which investigations are carried out, and introduce algorithmically provided rigor to ensure higher sensitivity and specificity of flagged transactions.

Additionally, there are data exchanges outside of the purview of CFIUS that also present a challenge to protection of US IP. For example, China does not permit its citizens' genomic data to be transferred outside national borders, yet the US currently permits Americans' genomic data to be sequenced by foreign biotech behemoths such as China-based BGI Group, which are often less expensive than US-based companies offering sequencing services[24]. Using a company like BGI Group may be beneficial from a monetary perspective, but sending such valuable data abroad leaves the US at a bioeconomic disadvantage. Thus, to protect genomic data while enabling free trade and an open economy, USG should investigate how distributed ledger technologies like blockchain[25], could be used to provide a firewall between the genomic data and the sequencing service being provided—in short, to enable companies like BGI Group to produce sequence data without gaining access to it.

Finally, to lessen cyber threats, USG should establish a testbed capability for evaluating cyber vulnerabilities in biotechnology equipment, software, databases, and information technology infrastructure associated with the bioeconomy. Such a clearing house could verify performance of tools against benchmarks in support of standard development, as well as identify and mitigate cybersecurity vulnerabilities[26]. Lessons learned from prior government-funded work can support the establishment and process development for this institution. NIST's National Cybersecurity Center of Excellence has ongoing efforts to identify genomic data cybersecurity and privacy concerns in support of the creation of effective industry guidance aimed to protect genomic data while enabling innovation. Furthermore, USG should promote to the stakeholder community models for disseminating information regarding biotechnology and biomanufacturing sector-targeted cybersecurity threats[27]. Existing efforts such as the MITRE ATT&CK framework and the Common Vulnerabilities and Exposures system could be leveraged for the biotechnology and biomanufacturing sector to collate a knowledge base of the observed tactics, techniques, and maneuvers of adversaries[28].

These immediate actions will reduce the threat of loss of intellectual property and cyber-physical attacks on biotechnology infrastructure by reducing cyber vulnerabilities and identifying possible direct or intangible technology transfers.

About the Authors

Dr. John Dileo manages the Biotechnology and Life Sciences Department at MITRE and has 20 years of experience in biomedical research and support to USG programs in biosafety, security, and countering weapons of mass destruction.

Dr. Kunal Rambhia is Group Leader for Medical Countermeasures at MITRE and has 15 years of experience in pandemic preparedness and response, science policy, tissue engineering, and advancing early-stage biotechnologies.

Dr. Matt Downs is a biomedical engineer whose research focuses on functional medical imaging, neuroscience, and material science. His recent work has included supporting injury-prevention standards, COVID-19 management and mitigation strategies, and synthetic biology efforts.

Dr. Janelle Rowell is a Senior Biotechnologist at MITRE where she supports government efforts to accelerate biomedical innovation and quick transition scientific discoveries to healthcare products that improve patient care and enhance health. She has a background in molecular medicine and experience in regulatory affairs.

Caroline Kennedy is a Biotechnologist and Project Leader at MITRE, where she has primarily supported work programs relevant to domestic and international biodefense, biosecurity, and One Health security. More recently, she has been involved in food and agricultural supply chain security and better understanding the domestic synthetic biology research ecosystem.

For more information about this paper or the Center for Data-Driven Policy, contact policy@mitre.org

References

[1] MITRE. [Online] Available https://portal.asias.aero/overview

[2] MITRE. [Online] Available https://attack.mitre.org/

[3] MITRE. [Online] Available https://cve.mitre.org/

[4] M. K. Mansoura and J. Schnitzer, "10-point action plan: sustaining a biopharma industrial base for a more secure nation." MITRE, 2021. [Online] Available: https://www.mitre.org/publications/technical-papers/10-point-action-plan-sustaining-biopharma-industrial-base

[5] R. A. Martin, "Trusting our supply chains: a comprehensive data-driven approach." MITRE, 2020. [Online] Available: https://www.mitre.org/sites/default/files/publications/pr-20-01465-37-trusting-our-supply-chains-a-comprehensive-data-driven-approach.pdf

[6] R. Hodge, R. A. Martin, and M. A. Aisenberg, "Supply chain security-it's everyone's business." MITRE, July 2021. [Online] Available: https://www.mitre.org/publications/technical-papers/supply-chain-security-its-everyones-business

[7] [Online] Available: https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/national_bioeconomy_blueprint_april_2012.pdf

[8] "Safeguarding the Bioeconomy." National Academies of Sciences, Engineering, and Medicine; Division on Engineering and Physical Sciences; Health and Medicine Division; Policy and Global Affairs; Division on Earth and Life Studies; Forum on Cyber Resilience; Board on Health Sciences Policy; Board on Science, Technology, and Economic Policy; Board on Agriculture and Natural Resources; Board on Life Sciences; Committee on Safeguarding the Bioeconomy: Finding Strategies for Understanding, Evaluating, and Protecting the Bioeconomy While Sustaining Innovation and Growth. January 14, 2020. doi:10.17226/25525o Accessed: April 18, 2022. [Online] Available: https://pubmed.ncbi.nlm.nih.gov/32352690/

[9] A. P. Hunger, G. Sanders, and S. Araz, "When biosecurity is the mission, the bioeconomy must become government's strategic partner." Center for Strategic and International Studies, July 19, 2021. Accessed: April 18, 2022. [Online] Available: https://www.csis.org/analysis/when-biosecurity-mission-bioeconomy-must-become-governments-strategic-partner

[10] "Safeguarding the Bioeconomy." National Academies of Sciences, Engineering, and Medicine; Division on Engineering and Physical Sciences; Health and Medicine Division; Policy and Global Affairs; Division on Earth and Life Studies; Forum on Cyber Resilience; Board on Health Sciences Policy; Board on Science, Technology, and Economic Policy; Board on Agriculture and Natural Resources; Board on Life Sciences; Committee on Safeguarding the Bioeconomy: Finding Strategies for Understanding, Evaluating, and Protecting the Bioeconomy While Sustaining Innovation and Growth. January 14, 2020. doi:10.17226/25525o Accessed: April 18, 2022. [Online] Available: https://pubmed.ncbi.nlm.nih.gov/32352690/

[11] B. Nogrady, "How Indian biotech is driving innovation." Nature, December 12, 2018. doi: 10.1038/d41586-018-07671-9 Accessed: April 18, 2022. [Online] Available: https://www.nature.com/articles/d41586-018-07671-9

[12] National Strategy Programs for Biotechnology and Genetic Engineering. http://www.eyas.eg.net/index.php/all-news/item/315-national-strategy-programs-for-biotechnology-and-genetic-engineering. Accessed March 23, 2022.

[13] "The next biotech superpower." Nature Biotechnology, Volume 37, Issue 1243, 2019. doi:10.1038/s41587-019-0316-7 Accessed: April 18, 2022. [Online] Available: https://www.nature.com/articles/s41587-019-0316-7

[14] 2019 Report to Congress of the U.S.-China Economic and Security Review Commission. 2019. [Online] Available: https://www.uscc.gov/annual-report/2019-annual-report-congress

[15] [Online] Available: https://portal.asias.aero/overview

[16] California Legislature. 2021-2022 Regular Session. September 9, 2021. AB-70 Gene synthesis providers. [Online] Available: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB70. Accessed March 23, 2022.

[17] [Online] Available: https://www.cisa.gov/critical-manufacturing-sector

[18] [Online] Available: https://www.cisa.gov/national-critical-functions-set

[19] National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience. Department of Homeland Security, 2013. Accessed: March 21, 2022. [Online] Available: https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

[20] A. Hope, "BIO-ISAC warns about Tardigrade Malware actively targeting biomanufacturing facilities." CPO (Chief Privacy Officers) Magazine, December 2, 2021. Accessed: April 18, 2022. [Online] Available: https://www.cpomagazine.com/cyber-security/bio-isac-warns-about-tardigrade-malware-actively-targeting-biomanufacturing-facilities/

[21] M. Hvistendahl, "China's theft of U.S. trade secrets under scrutiny." Science, February 28, 2017. Accessed: April 18, 2022. [Online] Available: https://www.science.org/content/article/china-s-theft-us-trade-secrets-under-scrutiny

[22] R. Respaut and J. Zhu, "As China builds biotech sector, cash floods U.S. startups." Reuters, September 23, 2018. Accessed: April 18, 2022. [Online] Available: https://www.reuters.com/article/us-biotech-china-investment/as-china-builds-biotech-sector-cash-floods-u-s-startups-idUSKCN1M400G

[23] MITRE, "10-Point Action Plan: Sustaining a Biopharma Industrial Base for a More Secure Nation." 2021 [Online] Available: https://www.mitre.org/sites/default/files/publications/pr-21-2355-10-point-action-plan-sustaining-biopharma-industrial-base.pdf. Accessed March 21, 2022. Accessed March 21, 2022.

[24] K. Needham and C. Baldwin, "China's gene giant harvests data from millions of women." Reuters Investigates: Baby Biocode, July 7, 2021. Accessed: April 18, 2022. [Online] Available: https://www.reuters.com/investigates/special-report/health-china-bgi-dna/

[25] B.A. Dedeturk, A. Soran, and B. Bakir-Gungor, "Blockchain for genomics and healthcare: a literature review, current status, classification and open issues." PeerJ, Volume 9, e12130, September 30, 2021. doi: 10.7717/peerj.12130 Accessed: April 18, 2022. [Online] Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8487622/

[26] "Safeguarding the Bioeconomy." National Academies of Sciences, Engineering, and Medicine; Division on Engineering and Physical Sciences; Health and Medicine Division; Policy and Global Affairs; Division on Earth and Life Studies; Forum on Cyber Resilience; Board on Health Sciences Policy; Board on Science, Technology, and Economic Policy; Board on Agriculture and Natural Resources; Board on Life Sciences; Committee on Safeguarding the Bioeconomy: Finding Strategies for Understanding, Evaluating, and Protecting the Bioeconomy While Sustaining Innovation and Growth. January 14, 2020. doi:10.17226/25525o Accessed: April 18, 2022. [Online] Available: https://pubmed.ncbi.nlm.nih.gov/32352690/

[27] "Safeguarding the Bioeconomy." National Academies of Sciences, Engineering, and Medicine; Division on Engineering and Physical Sciences; Health and Medicine Division; Policy and Global Affairs; Division on Earth and Life Studies; Forum on Cyber Resilience; Board on Health Sciences Policy; Board on Science, Technology, and Economic Policy; Board on Agriculture and Natural Resources; Board on Life Sciences; Committee on Safeguarding the Bioeconomy: Finding Strategies for Understanding, Evaluating, and Protecting the Bioeconomy While Sustaining Innovation and Growth. January 14, 2020. doi:10.17226/25525o Accessed: April 18, 2022. [Online] Available: https://pubmed.ncbi.nlm.nih.gov/32352690/

[28] MITRE ATT&CK®. [Online]. Available: https://attack.mitre.org/. Accessed March 23, 2022.

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®