P | I | P | S

Double Helix, Dual-Use

Securing Synthetic Biological Laboratories

PIPS White Paper 9.3: *Executive Summary*

Hali Czosnek, Research Fellow
Jared Bergen, Research Intern
Clara Waterman, Research Intern

The combination of gene-editing technology and dangerous pathogens could spur international pandemics. The likelihood of a security breach and subsequent epidemic of a genetically modified virus continues to rise. Through the Nunn-Lugar Global Program framework, the United States can apply its knowledge of securing nuclear and biological weapons facilities to laboratories. By physically securing laboratories and standardizing laboratory safety training, the United States can preempt deadly pandemics rather than reacting after a pandemic occurs.

Splicing Pathogens: A Security Threat

Pathogen splicing projects will become more popular as technology becomes cheaper and more accessible. The proliferation of pathogen-editing technology makes dual-use research cheaper and more accessible. One popular virus-editing technology is CRISPR-Cas9 because it is accurate, low cost, and easy to use. It is anticipated that the global CRISPR market will be worth more than $1.5 billion by 2022. As the barriers to entry decrease, pathogen-splicing technology will become more easily accessible to non-scientists outside of controlled laboratories.

- *Lab Failures Worldwide.* Between 2003 and 2015, 21 American labs failed to report laboratory incidents involving highly dangerous pathogens. Considering the United States currently has the best laboratory safety protocols, unreported or unknown security breaches in other countries are an even greater concern and threat to global public health.

- *Antibiotic Resistant Bacteria.* Gene-editing technology allows scientists to transform previously treatable strains of a bacteria into deadlier, antibiotic-resistant strains. A woman recently died as a result of a flesh-eating antibiotic resistant bacteria. Genetically modified antibiotic-resistant bacteria have the potential to kill millions, if not billions of people.

- *Deadlier Pandemics.* A pandemic version of avian flu (H5N1) is hypothesized to have a 60 percent case fatality rate; over half the world's population could die from the accidental or intentional release of the virus. The fatality rate only increases if avian flu is genetically modified to be transmissible through air droplets. No country has the necessary vaccines or public health protocols to handle a modified pathogen outbreak.

- *Infected Agriculture and Livestock.* Should a modified pathogen infect a livestock population, humans have the potential to also become infected. In 2010, anthrax was accidentally released from a Ugandan laboratory, infecting a nearby hippopotamus population. This outbreak led to the deaths of four people who consumed the infected meat. Future livestock infections involving genetically modified pathogens would cause mass devastation.

The most imminent threat comes from advanced laboratories capable of manipulating pathogens to make them more virulent. The combination of CRISPR, pathogens, and weak laboratory security standards creates a perfect storm for the next pandemic. The United States should take first steps to address the proliferation of gene-editing technology in these laboratories.

The Current Domestic and International Policies: A Patchwork Quilt

The current approach to managing pathogens is a patchwork of international and domestic policies. The Wassenaar Arrangement, Biological Weapons Convention (BWC), and the U.S. Nunn-Lugar Program are the three prominent policies. However, these policies overlook the emerging threat of pathogen manipulation in poorly secured laboratories worldwide.

- *Informal export control arrangements*. Wassenaar Arrangement is an informal export control group for dual-use technology between 41 countries. As Wassenaar is a non-binding arrangement, enforcement and monitoring of commitments is costly and not a common priority for states party to the treaty. Wassenaar fails to address the primary threat to U.S. security because the risk is not the dual-use technology itself, but a combination of the technology and naturally occurring pathogens.

- *Ineffective agreements with weak verification.* The Biological Weapons Convention is the first multilateral treaty that prohibits the "development, production and stockpiling of weapons of mass destruction." While a more robust alternative to the Wassenaar Agreement, the BWC lacks a thorough verification mechanism for monitoring state compliance with the treaty. The weaknesses of the Convention's framework and its failure

to address pathogen-editing research conducted in laboratories renders the BWC an incomplete policy to address current biosecurity threats.

- *Nuclear threat reduction initiatives.* The United States' Nunn-Lugar Global Program previously addressed nonproliferation and nuclear security concerns. The program successfully dismantled the nuclear capabilities of Ukraine, Kazakhstan, and Belarus following the former Soviet Union's collapse at the end of the Cold War. Nunn-Lugar subsequently expanded in 2003 to operate outside of the former Soviet Union, and broadened to include biological weapons. However, the Nunn-Lugar program has not dedicated serious attention to civilian lab and proper safety training.

Pandemic Prevention: Revisiting Nunn-Lugar

The United States represents the silver standard for laboratory security, making it the best actor to strengthen laboratory security. However, the United States would benefit from a gold standard for American laboratories and laboratories worldwide. This brief recommends a two-pronged approach for achieving the gold standard by expanding Nunn-Lugar. First, Nunn-Lugar could physically secure biological laboratories in the United States, and establish bilateral partnerships with foreign governments in order to strengthen laboratory security abroad. Second, standardize laboratory safety training through the Nunn-Lugar program to improve safety, security and efficiency within laboratories.

- *Physical security*. A necessary first step to prevent the release of a potential pandemic pathogen is to physically secure laboratories within Nunn-Lugar partner countries that conduct research genetically altering pathogens. Securing these laboratories is essential to mitigating the possibility of biological agents intentionally or accidentally exiting regulated spaces.

- *Standardized training*. Second, the Nunn-Lugar Global Program could provide standardized, in-person training to scientists working in laboratories capable of editing viruses and reducing the probability of a security breach. Nunn-Lugar's success in both physically securing facilities and training former weapons scientists demonstrates that it is the best vehicle for standardizing laboratory training in synthetic biology laboratories.

Conclusion

The expanded Nunn-Lugar Global Program is the United States' best and lowest-cost option for preventing the accidental release of genetically-modified viruses. Secure laboratories and

standardized training within domestic and international partner government laboratories are the first steps toward preparing for deadlier pandemics. Biological warfare might be inevitable by 2035, and the United States can never be too early or too prepared with the knowledge and safeguards in place to prevent a possible attack. Future policy projects should address the growing bio-terror threat that cannot be entirely controlled through improvements in laboratory security. However, laboratory security is one area which states can work to immediately improve. The only way for the United States to guard against a pandemic of epic proportions is to prepare for it today; these preparations begin with an upgraded Nunn-Lugar Global Program.