A biosecurity credential will create a well-trained, responsible workforce with a core set of skills necessary to secure the life sciences of the future.

PHOTO: ANNA SCHROLL/FOTOGLORIA/NEWSCOM

BIOSECURITY

Promoting biosecurity by professionalizing biosecurity

A credential system could improve policy and practice

By **Rebecca L. Moritz [1], Kavita M. Berger[2], Barbara R. Owen[3], David R. Gillum[4]**

New biotechnologies have the power to transform medicine, provide new sources of energy, and fill an expanding need for renewable, biologically derived products (the "bioeconomy"). But many of these powerful technologies and their products have the potential to be exploited for malevolent purposes or subverted to cause harm. Although many natural, accidental, and deliberate biological threats are governed by laws, agency- and national-level strategies, international instruments, guidance documents, and best risk management practices (*1*, *2*), these policies and practices are often based on a defined list of pathogens and toxins (*1*, *3*, *4*), do not necessarily mitigate the risks of the hazards, are not flexible to address new discoveries, may be political in nature, and may not keep pace with technological and workforce advances (*5*, *6*). We suggest that such limitations and variability in biosecurity policy and practice internationally could be addressed in part by enhancing and growing a workforce able to identify, assess, mitigate, and communicate security risks and solutions. We outline core competencies that such professionals should demonstrate and key steps needed to grow the profession by establishing a biosecurity credential.

Biosecurity is a multidisciplinary concept focused on keeping the researcher, public, and environment secure from the malicious exploitation of biological knowledge technologies and products (*7*). Biosecurity is distinct from securing other materials and technologies because biological organisms are found in nature, replicate, and can evolve through mutation, and much of the science and technology advances are developed in academia and industry throughout the world. Although biosecurity traditionally has focused on prevention, deterrence, and dissuasion of the development, production, and malicious use of microbes and toxins as weapons, it has expanded to include preventing the exploitation of knowledge, skills, technologies, and equipment to harm animals, plants, humans, and the environment. Life sciences researchers in academic and government institutions and bio-related industries are facing unprecedented security risks, including pathogens and toxins known to be harmful to public health and safety; unauthorized access to infectious materials in use, storage, and during transfer; culturing of pathogens from ancient reservoirs; synthesis of pathogens from published sequence data; and theft of data from and disruption of operations at biological facilities from cyber attacks. Adding to these concerns is the rapid progress of synthetic biology (for example, gene drives, synthesis of extinct viruses, creation of new pathogenic viruses, and production of chemicals in microbial systems), which presents new challenges to promote advancement while preventing malicious use.

Several positions at research, industry, health, law enforcement, security, and emergency response organizations are being asked to address different issues related to biosecurity. Yet although an individual may be delegated as the "responsible official" on paper, often requirements for a baseline level of biosecurity expertise do not exist. At the same time, many diverse professionals within an organization may have biosecurity as a component of their job yet may not be clearly designated as go-to biosecurity experts. Moreover, work in biosecurity has become, whether they fully realize it, the responsibility of every scientist and engineer working in the life sciences and with biological materials and/or data; every businessperson, entrepreneur, and venture capitalist working with life science products and information; and every life science explorer—including those in do-it-yourself biology (DIYBio) laboratories (*8*).

In our experience, we see a need for greater clarity and consistency in how to deal with biosecurity issues at many institutions (such as who to call, what to do, and what is considered dual use) and in different countries. For example, private and public institutions have documented incidents involving biosecurity breaches and/or lack

[1]University of Wisconsin–Madison, Madison, WI, USA. [2]Gryphon Scientific, Takoma Park, MD, USA. [3]Merck & Co., Inc., Kenilworth, NJ, USA. [4]Arizona State University, Tempe, AZ, USA. Email: rebecca.moritz@wisc.edu

of internal biosecurity controls that have resulted in use of pathogenic bacteria to deliberately harm co-workers; unauthorized importation of viral samples; and theft of scientific data, results, and technologies. We suggest that many policy efforts suffer from being too focused on mere compliance with policies ("checking the box") rather than on an enterprise- or system-wide approach to addressing biosecurity risks and threats. Biosecurity needs to become integral in many different professions and countries, highlighting the need for consistent and common understanding of capabilities for the prevention of such risks and threats.

Layered on top of this is a catch-22: Risk and threat management measures must recognize that our best defense to counter the malicious application of life science research relies in part on continued research, knowledge gain, and scientific and technology advancement. The solution can become the problem and the problem can become the solution—for example, the fundamental research to understand mechanisms behind transmission of influenza and coronavirus. Efforts to prevent malicious application of life science knowledge, skills, and technologies thus must be developed in a manner that does not unduly impede scientific progress to advance health, defense, agriculture, environmental health, science, and energy (*1*). Having individuals who are well versed in biosecurity and collaborate directly with researchers on a regular basis is critical.

PATHWAY TO PROFESSIONALIZATION

We suggest that a biosecurity credential based on core competencies could help ensure that professionals can address biosecurity gaps regardless of their home institution and collaborate with the life science community to mediate biosecurity risks in a manner that ensures continued advancement of life sciences research for the benefit of all. Such a credential must go beyond the governance of microbes and toxins and must consider the risks associated with the malicious use of synthetic biology, genome editing, genomics and health care data, neuroscience, and other enabling biotechnologies. Risks associated with digitization of biological information and networked systems also is included within the broader scope of biosecurity.

As the scope of biosecurity expands, the creation of a biosecurity credential would allow individuals from different disciplines, professions, backgrounds, and countries to be recognized by scientists, administrators, funders, and policy-makers as go-to resources for knowledge and expertise in the reduction of deliberate biological risks.

Establishing a biosecurity credential could provide individuals who are responsible for implementation and oversight of biosecurity practices at institutions with baseline knowledge about how to assess and address existing and new risks in their facilities, which promotes consistency in countering global biosecurity issues. A biosecurity credential should include, at a minimum, competencies that focus on biosafety, program management, physical security, personal security, personnel suitability, material control and accountability, transport security, cyber security, and information security (see the box) (*9*). These core competencies were identified by an exploratory task force led by the American Biological Safety Association (ABSA) International to cultivate a well-prepared biosecurity workforce. The task force had representation from academia, agriculture, government, private industry, public health, and security sectors. These core competencies were formulated on the basis of biosecurity lessons learned and shared experiences from this cross-functional task force.

Individuals who obtain a biosecurity credential may be subject-matter experts in one or more of these core competencies (some of which, such as biosafety and cyber security, have credentialing programs of their own). Obtaining a biosecurity credential would not require that an individual achieve expertise equivalent to a separate credential in each of the individual core competencies, but a credential would mean that an individual has substantial knowledge in all of the core competencies to be able to identify and remediate risks and to know whom to engage for deeper disciplinary expertise.

For a credential to be successful, the diverse international biosecurity community involved in biothreat reduction in high-, middle-, and low-income countries must be engaged to help identify specific areas relevant to their scientific, policy, infrastructure, and threat environments. Developing an assessment of core biosecurity competencies based on skills and knowledge that is not specific to one country is necessary for a successful and meaningful credential. Implementation may be as comprehensive as offering degrees from accredited institutions or as light as incorporating common norms and industry standards. For example, the implementation of the credential could be modeled after work being done within the DIYbio community, which involves obtaining widespread adoption of safety practices among distributed communities from around the world (*10*). This is an example of what can be achieved through engagement, communication, and partnership.

One possible first step could be to document current approaches for addressing each of the competencies at various institutions internationally. To the best of our knowledge, this has not been done systematically, and even within the United States there is a lack of clear and rigorous processes by which an individual develops knowledge and skills for practicing biosecurity. This step is critical for understanding current comprehension of each area, challenges in implementing long-term solutions, and lessons learned from past efforts. Together, this information helps to identify misconceptions about the core competencies, which would need to be addressed during development of the biosecurity credential. For example, the biosafety and biosecurity action package of the Global Health Security Agenda—an international effort to help countries develop capabilities for prevention of, detection of, and response to infectious disease threats such as Ebola virus and new coronavirus 2019 outbreaks—could provide an opportunity to compile a list of biosecurity practices that countries are developing and or implementing (*11*).

Another key step would be for stakeholders from different sectors, disciplines, and industries to come together to identify their needs and interest level for a biosecurity credential and to gain buy-in for assistance with the development and long-term implementation of the credential. There are multiple opportunities for international engagement. For example, the cooperative threat-reduction programs, international scientific organizations, and the Biological and Toxin Weapons Convention could support multisectoral discussions on the development of an international biosecurity credential and associated core competencies. This step is important for including that representatives from a variety of stakeholders are engaged, which ensures that the credential does not meet the needs of a subset of stakeholders at the expense (or even exclusion) of others. This step also promotes better understanding of biosecurity needs and resources among institutions, sectors, and countries, which is critical for sustainability and durability of the credential.

Documentation of risks and threats presented by different biological science and technology sectors and fields could help to ensure that the core competencies are relevant and applicable to past, current, and future risks and threats. For example, funding agencies, scientific journals, and the scientific and security communities could interact with governments of all countries to compile anonymized biosecurity lessons learned.

The concept of biosecurity has been a focus of several global initiatives, and many countries have supported efforts to build institutional, national, and regional capacity for biosafety and biosecurity and, to some

Biosecurity credential core competencies and examples of necessary knowledge and skills

Cyber security
Knowledge of protecting unauthorized access to computer networks involved in facility operation; equipment uses; and data generation, analysis, and storage

- Frameworks, methods, and technologies for protecting computers and facility control systems from cyber attacks and espionage
- Methods for encrypting documents for protecting information
- Methods for detecting, quarantining, and addressing malicious code
- Cybersecurity Framework of the U.S. National Institute of Standards and Technology

Information security
Knowledge about the methods to protect data and information associated with biological materials from unauthorized or accidental disclosure

- Different means of protecting data
- Identification and mitigation of vulnerabilities associated with data in transit and storage, including through access to software and cloud computing and storage

Program management
Ability to oversee the implementation of a comprehensive biosecurity program

- Risk assessment and risk management
- Knowledge of how to write and implement a biosecurity plan that addresses personnel management, physical security, material control and accountability, transport controls (such as locks, key card access, and/or biometric features), and cyber and data security

Personnel suitability
Knowledge regarding the actions and behaviors that lead to unauthorized access to materials and information resulting in theft, use, or release

- Best practices in personnel security
- Institutional and community entities involved in initial and ongoing vetting and evaluation of personnel for reliability and trustworthiness
- Awareness of elicitation techniques used to collect information without raising suspicion that certain facts are being sought
- Protections and processes for reporting insider incidents

Biosafety
Knowledge regarding containment principles and practices implemented to prevent accidental exposures and releases of biological materials

- Perform risk assessments, assign risk groups and containment levels, and design facilities to ensure safe work with biological materials

Physical security
Knowledge regarding the physical measures designed to prevent unauthorized access to facilities and equipment and theft of biological materials

- Various means of securing facilities and equipment
- Defining security zones with increasingly strict controls as you move toward an area where a high-risk agent is handled
- Using physical structures or barriers such as a gated property or access controls (such as locks, key card access, and/or biometric features)

Personal security
Knowledge regarding the risks to people with access to biological materials or associated information

- Guidance on how to train individuals on understanding their vulnerabilities to coercion or elicitation
- Knowledge of how to train individuals to be aware of threats to themselves, co-workers, workplace, and/or their families
- Processes and authorities to contact if an incident or suspected incident occurs
- Methods for protecting one's personal information and policies governing personally identifiable information or personal health information

Material control and accountability
Knowledge regarding the methods for inventorying and tracking high-consequence biological agents and toxins

- Various inventory and tracking systems
- Awareness of what materials exist, where they are located, and who is accountable for them
- Laboratory notebook accountability and archive programs, signature logs, inventories, and chain of custody policies

Transport security
Knowledge regarding systems in place to reduce the risk of theft during the transportation of materials from one area to another, between facilities within the same country, or from one country to another

- Chain of custody forms, package tracking, shipping regulations, permitting requirements, and surveillance options

extent, cyber and data security for biological facilities and information systems. We now see a credential system as a potential way to help strengthen and standardize ongoing international initiatives in biosecurity and incorporate emerging risks and cultivate a well-trained cadre of biosecurity professionals in a dynamic biotechnology landscape. ■

REFERENCES AND NOTES

1. D. DiEuliis, V. Rao, E. A. Billings, C. B. Meyer, K. Berger, *Health Secur.* **17**, 83 (2019).
2. World Health Organization (WHO), *International Health Regulations* (WHO, ed. 3, 2005).
3. The Biological Weapons and Toxins Convention includes microbes produced with genetic engineering or synthetic biology approaches, which broadens the scope of biological threats slightly.
4. K. M. Berger, *Science* **354**, 1237 (2016).
5. National Academies of Sciences, Engineering, Medicine, *Biodefense in the Age of Synthetic Biology* (National Academies Press, 2018).
6. J. B. Tucker, Innovation, *Dual Use, and Security. Managing the Risks of Emerging Biological and Chemical Technologies* (MIT Press, 2012).
7. In defense spheres, biosecurity refers to measures to prevent, deter, and dissuade efforts to develop, produce, stockpile, and use biological agents (pathogens and toxins) as weapons. The broader application of biosecurity includes prevention, deterrence, and dissuasion of usage of nonmicrobial or toxin-based biological material, biologically derived chemicals and small molecules, and data to harm others deliberately.
8. T. Kuiken, *Nature* **531**, 167 (2016).
9. R. Salerno, J. Gaudioso, *Laboratory Biosecurity Handbook* (CRC Press, 2007).
10. Baltimore Under Ground Science Space (BUGGS), a nonprofit public laboratory to safely and affordably investigate the living world; www.bugssonline.org/diybio-biosafety
11. Global Health Security Agenda (GHSA), https://ghsagenda.org

ACKNOWLEDGMENTS

D.R.G, R.L.M, and B.R.O. were members of the ABSA International exploratory biosecurity credentialing task force. D.R.G. is the 2020 president of ABSA International. B.R.O. and R.L.M. are former council members of ABSA International. K.M.B. serves as a deputy chair of the Global Health Security Consortium.

10.1126/science.aba0376

Promoting biosecurity by professionalizing biosecurity

Rebecca L. Moritz, Kavita M. Berger, Barbara R. Owen and David R. Gillum

Science **367** (6480), 856-858.
DOI: 10.1126/science.aba0376