BIORISK MANAGEMENT CASE STUDY: MASSACHUSETTS INSTITUTE OF TECHNOLOGY-BROAD FOUNDRY

Last Updated: September 20, 2022

SUMMARY

The MIT-Broad Foundry is a genetic design institute that developed methods for fast and large-scale engineering of genetic systems. The Foundry began as a collaboration between a university and research institute and received support primarily from U.S. government agencies, including the Department of Defense, and industry partners. The Foundry:

- sought to identify and manage risks associated with new technologies beyond those addressed in existing legal, federal, and institutional policies.
- created a culture of responsibility among staff by integrating a self-assessment tool into its routine operations and welcoming researcher participation in expert biosecurity review meetings.
- involved a broad set of stakeholders in biosecurity reviews including law enforcement, intelligence, defense, and policy experts as well as local physical and IT security professionals.

DISCLAIMER

Biosafety and biosecurity risk management practices can change over time. This case study represents one point in time and is a sample of an evolving set of risk management practices. For additional information on current practices please contact the organization directly.

Cite as: Gordon, B., Casini A., Salm, M., and Brink, K. (2023). Biorisk Management Case Study: Massachusetts Institute of Technology-Broad Foundry. Stanford Digital Repository. Available at https://purl.stanford.edu/mq491gw2822. https://doi.org/10.25740/mq491gw2822.

THE VISIBILITY INITIATIVE FOR RESPONSIBLE SCIENCE (VIRS)

The goal of the Visibility Initiative for Responsible Science (VIRS) is to share information about the value of biorisk management and how life science stakeholder organizations approach the issue. VIRS was conceived by a multi-stakeholder group during an April 2019 working group meeting of the Biosecurity Innovation and Risk Reduction Initiative (BIRRI) program of NTI Global Biological Policy & Programs. With support from NTI, Stanford University Bio Policy & Leadership in Society VIRS produced a set of Case Studies in biorisk management, and The Biorisk Management Casebook that provides cross-cutting insights into contemporary practices.

THE BIORISK MANAGEMENT CASE STUDIES

The Biorisk Management Case Studies describes biorisk management processes for a diverse set of life science research stakeholders. The collection serves to evaluate the feasibility and value of knowledge sharing among both organizations that have similar roles and those that have different roles in managing research. Case studies were developed in consultation with organizations through a combination of research based on public sources, interviews, and providing a template with guiding questions for organizations to complete directly. Additional analysis can be found in The Biorisk Management Casebook: Insights into Contemporary Practices[1] in this collection. Project Directors: Megan Palmer, Stanford University; Sam Weiss Evans, Harvard University.

CONTRIBUTORS

- Ben Gordon, Director, MIT-Broad Foundry
- Arturo Casini, Supervisor Research Scientist, MIT-Broad Foundry
- Melissa Salm, Stanford University
- Kathryn Brink, Stanford University

BACKGROUND OF ORGANIZATION

The MIT-Broad Foundry was a "genetic design institute that enabled the forward engineering of sophisticated massively multi-part genetic systems."[2] The Foundry began as a collaboration between a university (Massachusetts Institute of Technology (MIT)) and a research institute (Broad Institute), and it pioneered methods to design, build, and test engineer genetic systems quickly and at a large scale.[3] The Foundry applied these techniques to diverse engineering projects including chemicals, agriculture, materials, biomedicine, and control logic. The Foundry received much of its funding from the United States Department of Defense, including having received an initial five-year $32 million contract from the United States Defense Advanced Research Projects Agency (DARPA) in 2015.[2] The Foundry also received support from other U.S. government agencies and industry partners.

As a condition of its participation in DARPA's "1000 Molecules" program in 2015, the agency required the Foundry to implement a formal process for dealing with biosecurity concerns. While DARPA did not provide explicit guidance about how to implement such a process, the existence of this requirement propelled the Foundry to engage more deeply with biosecurity issues and look beyond standard institutional and legal biosafety measures.

Starting from a few individuals known to Foundry leadership, the organization recruited biosecurity experts to form a committee charged with developing policies for responsible research and evaluating biosecurity risks. Local stakeholders from the Broad Institute, such as facilities managers, were also invited to participate. The Foundry also encouraged representation from law enforcement (FBI), the intelligence community, and DARPA.

Once formalized as the Foundry's Biosecurity Advisory Committee (BAC), the committee used case studies to define policies and operating procedures, which ultimately included preventive measures and routes for escalating concerns. Since its founding, the committee became a central part of Foundry operations, and as detailed below, one of its greatest impacts was fostering an organization-wide culture of responsibility among all researchers in the group.

PROCESS

Scope of risks considered

The BAC leveraged the broad expertise of its members to define areas of concern and risk categories for consideration. The BAC focused on potential biosafety and biosecurity issues not addressed by established law or institutional, sponsor, or government policies, with a particular emphasis on risks enabled by new technologies discovered at the Foundry. One fundamental concern was that technological advances lower the barrier to building biological systems, including potentially dangerous ones. This increases both the number and types of actors that can use these systems and with their ability to affect the world. For example, the dissemination of information on how to biosynthesize certain therapeutics might also facilitate the biosynthesis of chemically similar illicit substances. Other advances could potentially facilitate the deployment of engineered biological systems outside laboratory environments, where containment and monitoring are significantly more challenging. Currently, biological surveillance systems are quite limited in their scope and accuracy since they primarily focus on controlling access to human pathogens and nucleic acid molecules encoding their genes. As a result, emerging risks that do not fall into these categories might be overlooked. The difficulty of enforcing effective surveillance on emerging risks is compounded by the fact that technology development typically involves multiple academic and commercial entities that each have their own policies, and that treat information, intellectual property, patient consent, and international treaties differently.

At a high level, the Foundry considered two types of risks: technological risks and access risks.

Technological risks are risks associated with the development of a new technology, including both risks from the (mis)application of a specific technology and risks from the development of broadly applicable methods that may reduce the barrier to misuse. Additionally, a distinction is made between risks that arise only after a project is complete and risks that are present during the development of a project.

The Foundry further divides technological risks based on the areas of concern defined by the BAC, which include:

- Effects on public health
- Effects on the environment
- Dual-use potential for weaponization
- Societal or economic effects
- Effects on the operation of the Foundry (e.g., facility security, such as risks to instrumentation)
- Other

Access risks relate to projects that present risks in case of unauthorized access to information or materials. A distinction is made between intrusion events by outsiders (e.g., external threats) and unauthorized access by individuals internal to the Foundry or their collaborators (e.g., insider threats). Access risks encompass both unauthorized access to physical materials stored in the Foundry laboratories and to documents or data stored on computers and servers (information technology, IT).

Overall sequence of steps

The Foundry performed risk assessment and mitigation through two main processes: (1) self-assessment with peer review at lab meetings and (2) formal review by the BAC.

Like many academic research laboratories, the Foundry held weekly lab meetings, during which one or two members of the group presented their progress to their colleagues. These weekly meetings rotated between different researchers and research projects, such that every member of the group provided an update every 3-6 months. At the end of each lab meeting, the presenter was asked to show a biosecurity risk self-assessment slide for the project (see Appendix A). This slide served as the basis for a free-form discussion among Foundry research staff about the biosecurity risks associated with the project, both at the meeting and in informal follow-on discussions.

Individual projects were then formally reviewed one to two times per year by the BAC, using the self-assessment slides for reference. Projects were presented to the BAC by the Foundry director. With this schedule, most projects were reviewed within 3-6 months of inception, and on occasion, projects in the proposal stage were also discussed. If any concerns arose between committee meetings, the Foundry director could also bring projects directly to the attention of the committee or committee chair for immediate consideration. Researchers at the Foundry were invited and encouraged to attend these meetings, with some self-selecting to do so. Participating in committee meetings helped to provide researchers with context for why biosecurity is important and exposed them to the way that biosecurity and biosafety experts assess and mitigate risks, which in turn helped improve the quality of the free-form discussions of the self-assessment slides.

Risk assessment

The Foundry did not undertake any projects with obvious biosecurity risks (e.g., projects involving the use of select agents), so its primary motivation was in identifying non-obvious concerns. It did this by establishing a rubric to guide researchers and members of the BAC as they explored potential risks, as listed in the "Scope of risks considered" section. Structuring the evaluation process also made it more accessible to researchers.

This rubric took the form of a risk-assessment matrix in a PowerPoint slide format (see Appendix A). The matrix comprises two tables, in which each cell can be filled in with a yes/no response to indicate whether the project might pose a particular kind of risk. For any "yes" entries, text fields were provided for documenting the rationale. This rubric was employed by everyone in the research group, including the BAC, leadership, and individual researchers. Leadership used the rubric when considering new projects and proposals, the BAC used the rubric during project review, and perhaps most powerfully, individual contributors in the lab used the rubric to perform self-assessments when preparing to formally present their technical progress to their peers. To build a culture of biosecurity awareness and personal responsibility throughout the laboratory and to encourage discussion of risk considerations, researchers were required to complete the rubric template and to incorporate the slide into their periodical presentations.

When presenting their self-assessment to their peers and to Foundry leadership, researchers were encouraged to convey their concerns (if any), explain their reasoning (even if none), and ask for help and feedback. Leadership also helped to catalyze engagement across the room, especially in cases that were difficult to evaluate. Sometimes the discussion organically took the form of red teaming in which the group envisioned ways that the methods developed for a project or its resulting technologies could be misused. In many cases, these discussions would focus on how plausible the identified misuse scenarios were, often drawing on the project's similarity to previous self-assessments of other projects. Many of the possible risks identified through these

discussions were assessed to be unlikely to be realized or only relevant on very long timescales. For projects with more immediate or likely risks, discussions also involved identifying potential mitigation strategies. Following the presentation, slides would be updated based on the discussion.

The self-assessment slides also served as a record of projects that were made accessible to biosecurity experts on the BAC. As such, they were used as the basis for project review during the BAC's regular meetings. These review meetings consisted of three parts: (1) an overall update on ongoing work at the Foundry, (2) a review of projects with possible security concerns, and (3) a broader discussion about security issues in a topic area relevant to the Foundry's research. The project review part of the meeting covered both research projects that were in progress and research proposals that were in development. During project review, the Foundry director summarized questions that had arisen about a project (e.g., through self-assessment slides and associated discussions). The committee discussed the risks amongst themselves and suggested mitigation measures. While the committee served an important advisory function, the MIT-Broad Foundry director ultimately made a decision about whether and how a project would (or would not) proceed.

Risk mitigation

Even prior to reviewing any specific research projects, the BAC attempted to elaborate a set of potential mitigation strategies they might use if a project posed certain types of security risks. Broadly, these fell into two categories: stopping a research project entirely or stopping an aspect of a research project.

Specific mitigation measures employed at the Foundry included:

- Altering or limiting the technical focus of a project
- Adding additional cybersecurity and/or physical security protections to the materials or data associated with a project
- Consulting with external experts, including attorneys, policy experts, and law enforcement
- Considering how the public will respond to the project
- Suspending or ending a project

Other mitigation measures considered by the Foundry included:

- Accelerating the schedule for reviewing a project
- Sharing information regularly with relevant parties, such as security or law enforcement
- Imposing requirements on collaborators
- Including an additional project component, such as building safeguards or developing monitoring capabilities
- Developing a publication policy, including limiting publication of methods or results and/or early publication of the intended approach to get feedback or spark discussion
- Engaging in discussions with stakeholders for projects that could be controversial
- Declining funding from a source if the source was not committed to responsible research

Expertise required

The BAC included policy experts (mostly university professors), synthetic biologists, law enforcement (including both federal and regional representatives), international safety and security experts, United States government defense and intelligence community members, and staff of the institute where the Foundry was located (e.g., representatives from information technology (IT) security, physical plant security, head of biosafety). While most committee members were involved because of their direct biosecurity expertise, local members with expertise in IT and physical security played an important role in assessing and managing risks specific to Foundry data, materials, and infrastructure. All positions were volunteer.

IMPACT

The process of reviewing and addressing potential biosecurity risks by the BAC was typically beneficial for the projects. The burden imposed on the researchers via the self-assessment form was low, and in the rare cases where concerns were identified and mitigation measures were taken, these did not compromise the overall goals of the projects. These measures rather let the researchers continue their projects with the confidence of having properly addressed any biosecurity concerns and thus without worrying about running into obstacles in the future, for example when disseminating their work.

Overall, the Foundry successfully developed a culture of responsibility through the Foundry's self-assessment generation and discussion processes. Researchers were proactive about identifying and discussing security concerns in their work and were amenable to modifying a project in response to concerns. Nevertheless, sustaining this culture required effort: newly hired researchers were often unaware of biosecurity concerns and not trained in evaluating them, so they needed to be introduced to the process of self-assessment and group discussion. On the other hand, researchers in charge of the longer-running projects that had gone through multiple rounds of the self-assessment process tended to struggle to maintain engagement due to its inherent repetitiveness, which was addressed by Foundry leadership through regular reminders and support during group discussions.

FEEDBACK

One of the greatest challenges in developing the Foundry's risk management process was defining a self-assessment process that would be effective in the hands of the researchers. Informal feedback collected directly from the researchers at the Foundry showed that for most of them the biosecurity self-assessment matrix (Appendix A) was difficult to understand because they were not familiar with the concept of biosecurity risk and its different subtypes. The issue was tackled by periodically giving the researchers a brief primer on biosecurity risks as an oral presentation by Foundry leadership during group meetings, explaining these concepts with examples. Additionally, the matrix went through minor modifications implemented by Foundry leadership following discussion with the BAC (e.g., removing the distinction between "interest" and "vulnerability" for intrusion risks), and notes were added on the matrix itself as an easily accessible reference to clarify the meaning of key terms (e.g., "methods" vs "applications," and "in development" vs "complete"). Early in its history, the BAC emphasized that Foundry practices be adaptive, so small changes (such as these) and large changes (such as establishment of the rubric in the first place) were consistent with lab culture.

SHARING

The Foundry shared its approach to assessing and managing biosecurity risks on multiple occasions by giving public talks at scientific conferences and at specialized meetings (e.g., Three I's: Biosecurity & Research Integrity 2019). The main purpose of these talks was to encourage wider adoption and to receive feedback on these practices. Reception has consistently been very positive, and in multiple instances members of the audience asked for a copy of the self-assessment matrix for their own use.

The Foundry has refrained from sharing biosecurity self-assessment information about specific projects publicly because these assessments can contain sensitive information about potential biosecurity risks. These were only shared with committee members or with external individuals as needed.

REFLECTIONS

The Foundry offers the following reflections on their risk management practices:

- The mechanisms the Foundry put in place to foster a culture of responsibility involving all researchers in the lab - notably requiring biosecurity self-assessments, weekly discussions about biosecurity risks, and annual or biannual meetings with experts open for researchers to attend - should be replicable in other research environments. The Foundry welcomes broader adoption of these practices.
- There are many security risks that exist beyond those captured in traditional biosafety and biosecurity risk assessments (e.g., pathogens and toxins). Encouraging researcher participation and using discussion-based approaches to risk assessment enabled the Foundry to take a comprehensive approach to biosecurity and to identify risks that might otherwise go unrecognized.
- Assembling a committee with the appropriate expertise to manage biosecurity risks can be challenging; it is difficult to know who to ask for some security questions. Given the unique access Foundry leadership had to a handful of biosecurity experts, the Foundry's BAC model may not be easily replicable in other organizations. Instead, an Institutional Biosafety Committee (IBC) model could be a useful starting point. A biosecurity-specific review board should also include members of law enforcement and government to be maximally effective, as identifying

certain risks requires thinking creatively about issues that are not in the purview of scientists (e.g., crime, terrorism, international diplomacy). Developing formal and standardized structures for managing biosecurity concerns could also facilitate knowledge sharing between organizations about their experiences.

- It is useful to have a primer available, either as a written document or as a slide deck for presentation, that can be used to introduce the basic concepts of biosecurity risk to researchers that have not been exposed to these previously. This helps prevent both (i) the issue of not being able to recognize risks effectively and (ii) that of seeing risks in all projects (i.e., the "plastic fork" analogy: a plastic fork could be used to cause harm, but ultimately is extremely limited in the harm that it can cause and may not warrant mitigation measures).
- Defining an appropriate frequency for the self-assessments and the appropriate person responsible for them for each project is critical for their effectiveness. These change depending on the type of project and on the structure of the lab. If too infrequent, self-assessments can allow too much time to pass before risks are recognized. If too frequent, engagement with the process can be reduced due to its repetitiveness. Ideally, the person responsible for the self-assessment should be aware of both the larger context of the project and all the details of its experimental design. If a single such person does not exist, the responsibility of self-assessment might be shared among multiple individuals.
- Managing the dissemination of information about potential security risks while also encouraging experts and researchers to engage in informal, small-scale red-teaming exercises has been challenging. Researchers have found it awkward at times to manage this balance. When engaging external experts, Foundry leadership is careful about who it consults, relying on recommendations from trusted contacts. Looking forward, because it is possible that new biotechnologies may touch on sensitive areas, it will be important to have access to experts who are able to accept controlled information.

REFERENCES

1. Greene, D., Brink, K., Salm, M., Hoffmann, C., Evans, S. W., and Palmer, M. J. (2023). The Biorisk Management Casebook: Insights into Contemporary Practices. Stanford Digital Repository. Available at https://purl.stanford.edu/hj505vf5601. *https://doi.org/10.25740/hj505vf5601.*

2. Casini, A. *et al.* A pressure test to make 10 molecules in 90 days: external evaluation of methods to engineer biology. *Journal of the American Chemical Society.* 26 Feb 2018.

3. Mertz, L. The Foundry: Scaling Up Biological Design. *IEEE EMBS Pulse.* 27 Apr 2016. *https://www.embs.org/pulse/articles/the-foundry-scaling-up-biological-design/*

APPENDIX A:
MIT-BROAD FOUNDRY BIOSECURITY RISK SELF-ASSESSMENT

Biosecurity Risk Self-Assessment Matrix

Project Title:
Researcher/Team:
Project Aims:

Technological Risks

	APPLICATIONS		METHODSA	
	IN DEVEL[B]	COMPLETE	IN DEVEL[B]	COMPLETE
public health	–	–	–	–
environment	–	–	–	–
weapons	–	–	–	–
societal or economic	–	–	–	–
Foundry operational	–	–	–	–
other	–	–	–	–

Access Risks During Development

	INTRUSION	INTERNAL[C]
physical	–	–
IT	–	–

a **"Methods"** are the new methods/technologies that your project is developing (not the methods you use to do the work).
b **"In development"** refers to risks we could incur before and during project work, as opposed to risks that are only relevant once the project is complete
c **"Internal"** includes collaborators