CALL FOR PAPERS

First International Workshop on Cyberbiosecurity (CyberBio 2026)

Workshop proposal submitted to IEEE Symposium on Security and Privacy 2026
May 21, 2026 | San Francisco, CA, USA

Overview

The convergence of digital technologies and biological systems is driving the bioeconomy while introducing novel security risks that extend beyond traditional cybersecurity. **The First International Workshop on Cyberbiosecurity (CyberBio 2026)** brings together researchers, practitioners, and industry leaders to address the emerging security challenges at the intersection of cybersecurity and biological systems. As the bioeconomy increasingly relies on digital infrastructure, from DNA synthesis and laboratory automation to bioinformatics and supply chain management, new attack surfaces emerge that require specialized security frameworks transcending traditional cybersecurity boundaries. There is an growing need to adapt cybersecurity practices for biological systems.

This workshop focuses on protecting biological research, biomanufacturing, and bioeconomic infrastructure from digital threats and on promoting secure-by-design approaches for emerging biotechnologies. It is a premier forum fostering collaboration between the cybersecurity community and biotechnology stakeholders.

Topics of Interest

We invite submissions on all aspects of cyberbiosecurity, including but not limited to:

Security of Biological Infrastructure

- Authentication and authorization for laboratory equipment and automated systems
- Secure communication protocols for biomanufacturing networks
- Zero-trust architectures for biotechnology environments
- Physical-digital security for biocontainment facilities
- Supply chain security for biological materials and reagents

AI Safety in Biotechnology

- Adversarial attacks on machine learning models in biological applications
- Safety alignment for AI-driven protein design and metabolic engineering
- Formal verification methods for bio-AI systems
- Information hazard management in AI-accelerated biological research
- Robustness testing for biological discovery models

Data Protection and Privacy

- Genomic data security and privacy-preserving computation
- Secure storage and transmission of biological research data
- Anonymization techniques for biological datasets
- Consent and governance frameworks for biological data sharing
- Intellectual property protection in collaborative biological research

Threat Detection and Response

- Anomaly detection in biological data streams and laboratory workflows
- Forensic analysis techniques for cyber-bio incidents
- Incident response protocols for biotechnology organizations
- Attribution methodologies for attacks on biological infrastructure

- Threat intelligence sharing for the bioeconomy

DNA Synthesis and Screening Security

- Vulnerabilities in nucleic acid synthesis screening systems
- Cryptographic protocols for DNA synthesis order verification
- Advanced screening techniques resistant to AI-generated sequences
- Secure multi-party computation for sequence analysis
- Blockchain-based traceability for synthetic biological materials

Regulatory and Policy Frameworks

- Cybersecurity requirements for biotechnology compliance
- International cooperation on cyberbiosecurity standards
- Risk assessment frameworks for bio-cyber systems
- Ethics and dual-use considerations in cyberbiosecurity research
- Legal and regulatory responses to cyberbiosecurity incidents

Case Studies and Threat Analysis

- Analysis of real-world cyberbiosecurity incidents
- Threat modeling for specific biological systems or organizations
- Red team exercises and penetration testing in biotechnology environments
- Economic impact analysis of cyberbiosecurity threats
- Lessons learned from traditional cybersecurity applied to biological systems

Information for Authors

Contribution Categories

- **Full Papers (6-10 pages):** Original research contributions with comprehensive evaluation
- **Short Papers (up to 5 pages):** Work-in-progress, preliminary results, or focused contributions
- **Industry Papers (up to 5 pages):** Practical experiences, deployed solutions, or industrial case studies
- **Position Papers (up to 5 pages):** Vision statements, outstanding challenges, or perspectives on future directions
- **Presentation abstracts (up to 2 pages):** Prominent cyberbiosecurity papers recently accepted elsewhere

Submissions

- Submissions should be uploaded to the workshop submission system at: <EasyChair URL to be provided>
- At least one author of accepted papers must register for and attend the workshop to present the paper
- Submissions of papers should not substantially overlap with papers published or under review at other venues. Accepted papers will appear in the IEEE CS Press published proceedings.
- Presentation abstracts may report findings that were published or are about to be published elsewhere. Presentation abstracts will appear on the workshop website and will not be included in proceedings.

Review Process

- All submissions will undergo rigorous peer review by program committee members
- Review criteria include technical quality, originality, relevance to cyberbiosecurity, clarity, and dual use. During submission authors must flag potential dual use such as possibly

actionable biological protocols, sequence-level exploit details, or other sensitive artifacts. Qualified PC members will review sensitive artifact and provide instructions to reduce risk if needed.
- Authors will receive detailed feedback regardless of acceptance decision

Important Dates

All deadlines are 23:59:59 AoE (UTC-12)

- **Paper Submission Deadline:** January 30, 2026
- **Notification of Acceptance:** February 27, 2026
- **Camera-Ready Papers Due:** April 10, 2026
- **Workshop Date:** May 21, 2026

Workshop Organizers

General Chair

- **Whitney Bowman-Zatzkin**, BIO-ISAC, USA

Program Committee Chairs

- **Prof. Rami Puzis**, Ben-Gurion University of the Negev, Israel
- **Dr. Jacob Beal**, RTX BBN Technologies, USA

Publicity and External Relations Chairs

- **Prof. David Molik**, Kansas State University, USA
- **Tessa Alexanian**, International Biosecurity and Biosafety Initiative for Science (IBBIS)

Program Committee

The workshop program committee includes leading experts from cybersecurity, biotechnology, and policy communities representing academia, industry, and government organizations worldwide. (Full list will be available on the workshop website)