AFRL-SA-WP-TR-2020-0013

Operations Security for Emerging Biotechnology Applications

Jameson D. Voss[1], Erin M. McAuley[2], Ezekiel J. Maier[2], Michelle Rozo[3], Richard R. Chapleau[4], Albert H. Bonnema[4], Alexander J. Titus[5,6]

[1] United States Air Force Medical Readiness Agency, Defense Health Headquarters, Falls Church, VA 22042, USA
[2] Booz Allen Hamilton, Inc., McLean, Virginia 22102, USA
[3] Office of the Under Secretary of Defense for Research & Engineering, Pentagon, Washington DC 20301, USA
[4] United States Air Force School of Aerospace Medicine, Public Health & Preventive Medicine Department, Wright-Patterson AFB, Dayton, OH, 45433, USA
[5] Advanced Regenerative Manufacturing Institute, Manchester, NH, 03101, USA
[6] University of New Hampshire, Manchester, NH, 03101, USA

September 2020
Interim Report

Air Force Research Laboratory
711th Human Performance Wing
U.S. Air Force School of Aerospace Medicine
Public Health Department
2510 Fifth St., Bldg. 840
Wright-Patterson AFB, OH 45433-7913

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

Qualified requestors may obtain copies of this report from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-SA-WP-TR-2020-0013 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

//SIGNATURE//	//SIGNATURE//
COL BRETT R. NISHIKAWA	COL MONICA U. SELENT
Chief, Applied Technol & Genomics Div	Chair, Public Health Department

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
30-11-2020	INTERIM	01-01-2018 – 31-12-2019

4. TITLE AND SUBTITLE

Operations Security for Emerging Biotechnology Applications: BioOPSEC to Address Biotech Security

5a. CONTRACT NUMBER
B0900-0521/0050

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Jameson D. Voss, Erin M. McAuley, Ezekiel J. Maier, Michelle Rozo, Richard R. Chapleau, Albert H. Bonnema, Alexander J. Titus

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Jameson D. Voss[1], Erin M. McAuley[2], Ezekiel J. Maier[2], Michelle Rozo[3], Richard R. Chapleau[4], Albert H. Bonnema[4], Alexander J. Titus[5,6]
[1] United States Air Force Medical Readiness Agency, Defense Health Headquarters, Falls Church, VA 22042, USA
[2] Booz Allen Hamilton, Inc., McLean, Virginia 22102, USA
[3] Office of the Under Secretary of Defense for Research & Engineering, Pentagon, Washington DC 20301, USA
[4] United States Air Force School of Aerospace Medicine, Public Health & Preventive Medicine Department, Wright-Patterson AFB, Dayton, OH, 45433, USA
[5] Advanced Regenerative Manufacturing Institute, Manchester, NH, 03101, USA
[6] University of New Hampshire, Manchester, NH, 03101, USA

8. PERFORMING ORGANIZATION REPORT NUMBER

AFRL-SA-WP-TR-2020-0013

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
United States Air Force Medical Readiness Agency, Defense Health Headquarters, Falls Church, VA 22042

10. SPONSORING/MONITOR'S ACRONYM(S)
USAFSAM/PHT

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-SA-WP-TR-2020-0013

12. DISTRIBUTION / AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited. 88ABW-2020-0070, cleared 12 August 2020

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Widespread collection, distribution, and storage of biotechnological data in global collaborations continue to contribute to remarkable advancements in human health. However, widespread biomedical data collection also precipitates emergent vulnerabilities in data security, individual privacy, and scientific reproducibility. Mitigating vulnerabilities in biotechnological infrastructure and workflows requires engagement and collaboration amongst all stakeholders, which can be accelerated via use of standardized security procedures and terminologies. Herein we present Biotechnological Operations Security (BioOPSEC), an extensible framework that unifies the terminologies and concepts between biological, cyber, network, and physical security siloes. Additionally, by integrating biotechnology-specific considerations, BioOPSEC can be applied across the disparate systems, equipment, experimental procedures, operators, and environments in which biotechnological data are utilized. BioOPSEC identifies and analyzes existing best practices, novel vulnerabilities, and high-impact countermeasures for biomedical data procurement. In order to demonstrate the BioOPSEC process, we simulate a multi-site precision medicine study in order to analyze the potential chain of custody of a genomic biospecimen. For each step in the genomic biospecimen lifecycle, we identify critical information, analyze threats and vulnerabilities, assess risk, and prioritize countermeasures.

15. SUBJECT TERMS
operations security, genomic data, privacy, security, data integrity

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Richard R. Chapleau
U	U	U	SAR	18	19b. TELEPHONE NUMBER *(include area code)*

This page intentionally left blank.

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

1.0 EXECUTIVE SUMMARY

Responsible biotechnology research optimizes opportunities while deterring nefarious exploitation. New opportunities to collect and store biological attributes in global collaborations lead us to confront some emergent vulnerabilities for the first time. These tradeoffs warrant a comprehensive analysis of risks to data integrity, individual privacy, and national security. The military balances operational requirements and security using principles of "Operations Security." We adapt these principles to biotechnology in "BioOPSEC" as an extensible framework that unifies the terminologies and concepts between biological, cyber, network, and physical security siloes. As a result, BioOPSEC promotes existing best practices, proactively identifies new vulnerabilities, and deploys prioritized countermeasures. As OPSEC compels information sharing with friendly forces, BioOPSEC also promotes adoption of interoperable technical solutions that expand role-based access. Using precision medicine research as an example implementation, we demonstrate that BioOPSEC is agnostic of data type, environment, and operator and as such, can be broadly adopted across the bioeconomy. Our contribution here is expected to inform ongoing discussions about fostering biotechnology development in the midst of security considerations.

Research Innovation and Objective: In order to use sensitive biomedical data to benefit service member health, performance and readiness, it is critical to enable secure storage of the data and address military-specific privacy requirements and national security concerns. Information protection is uniquely important for the military and so a thorough, multidimensional systems analysis process is used to address vulnerabilities in security while supporting friendly information operations. To address these gaps, we sought to establish a balanced, multidimensional systems analysis process that could be applied by the biotechnology community to protect biomedical data procurement, storage, and use.

2.0 ***Impacts on Warfighter Mission:*** **Widespread collection of biomedical data is critical for increasing the clinical utility of biotechnology research and development. The balance of safeguarding those biomedical data from adversaries and supporting friendly operations is of utmost importance for protecting the warfighter, the unit, and the mission. Moreover, appropriately balancing these trade-offs will optimize opportunities to transform biotechnology research into more efficacious healthcare solutions for the warfighter and force health protection.**

2.0 INTRODUCTION

2.1 Privacy and Security Considerations of Genomic Data Collection

Rapid advances in biotechnology are driving significant growth across applications in energy, health and medicine, food and agriculture, environmental, and industrial sectors (https://roadmap.ebrc.org/). The biotechnology research enterprise includes a wide range of disciplines and significantly contributes to the global bioeconomy.[1] While data sharing platforms for genomic, health, and industrial data hold promising opportunities for precision medicine[2], their widespread use presents unprecedented vulnerabilities in data privacy and security. One such vulnerability is re-identification of data providers, due to the growing amount of publicly available electronic data and the sophistication of tools with which to analyze such data. Recent work has demonstrated that a disease allele, disease status, or a portion of a target's genome can be reconstructed without using genomic material from the target.[3], [4] Individual loss of genomic privacy is not reversible, and can affect a specific individual, family, and offspring. Collective loss of genomic privacy, in which an entire U.S.-based database is compromised by an adversary, could result in re-identification of many Americans, even those not in the database.[5]

Current privacy regulations do not wholly address these concerns in the digital and global biotechnology enterprise (**Figure 1**). The main legislation for healthcare privacy, the Health Insurance Portability and Accountability Act (HIPAA), aims to protect de-identified data via access control. However, aggregation or de-identification is often insufficient to prevent privacy violations.[6], [7] Furthermore, HIPAA does not cover data generated or disclosed outside of covered entities or U.S. jurisdiction. User-generated digital data (such as direct-to-consumer genomics sequencing[8], mobile applications, wearable devices, health-related Google searches or shopping patterns, social media posts, etc.[9]) are also outside the scope of HIPAA. In terms of international data sharing, the Foreign Investment Risk Review Modernization Act (FIRRMA)[10], permits the review and blockage of investments in U.S. critical infrastructure, technology, or personal data to protect data exposure to foreign governments.[11] However, FIRRMA's jurisdiction is limited and subject to non-binding legislation.

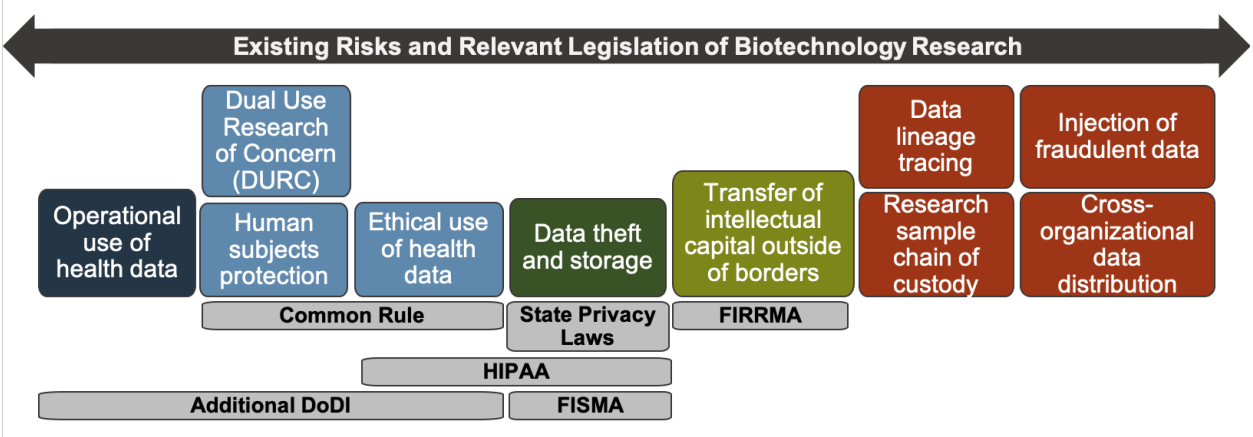

Figure 1: Relevant Regulatory Frameworks for Addressing Ethics and Security Risks Associated with Biotechnology Research. More traditional risks of collection and storage of health data (shown in blue and green) are at least partly addressed by legacy-based legislation. Emergent risks, shown in red, are not adequately covered by existing legislation. This gap is especially for biotechnology which is "thoroughly dual-use" meaning there are both public and private sector applications that can be either responsible or

nefarious. In the military, DoD-specific Instruction (DoDI) have been established to support additional ethics, individual, and national security reviews for human subjects research in active duty military personnel.

It can be difficult for dissimilar organizations to fully consider or vet individual and national trade-offs of genomic data sharing. A threat model for genomic data is under-developed, and as opportunities for utilizing genomic data expand, the risks and effects of data breach will likely increase. Therefore, a thorough characterization of the dynamic threat landscape is required. Historically, the Department of Defense has championed biotechnology research to improve performance, medical readiness, and force health protection.[12]–[14] The Department of Defense has a documented track-record and distinct interest in ongoing vulnerability assessments of privacy and security risks within the biotechnology enterprise.[15]

As these considerations apply to a broad audience, we present Biotechnological Operations Security (BioOPSEC), a structured and extensible analysis tool for proactive identification of security vulnerabilities throughout biotechnology data procurement, use, and sharing. BioOPSEC is well-suited to address tradeoffs and barriers to information utilization among multiple agents (ranging from friendly to adversarial) in a complex system. Importantly, BioOPSEC unifies terminologies, safeguards, and specialized operators, particularly within biological, cyber, network, and physical security.

2.2 Introducing BioOPSEC: A Framework for Evaluating Risks and Applying Countermeasures

The BioOPSEC framework is adapted from the military OPSEC.[33] Information protection is important for the military and so a thorough, multidimensional systems analysis process is used to address vulnerabilities in security while supporting friendly information operations.[15, p. 3] The process relies on personnel of all expertise to understand OPSEC concerns and proactively participate in continuous risk mitigation, often in conjunction with embedded security experts. BioOPSEC applies core principles of OPSEC within the context of biotechnology systems, equipment, experimental procedures, operators, and disparate environments[16] in which data are collected or biotechnology is utilized (**Figure 2**).

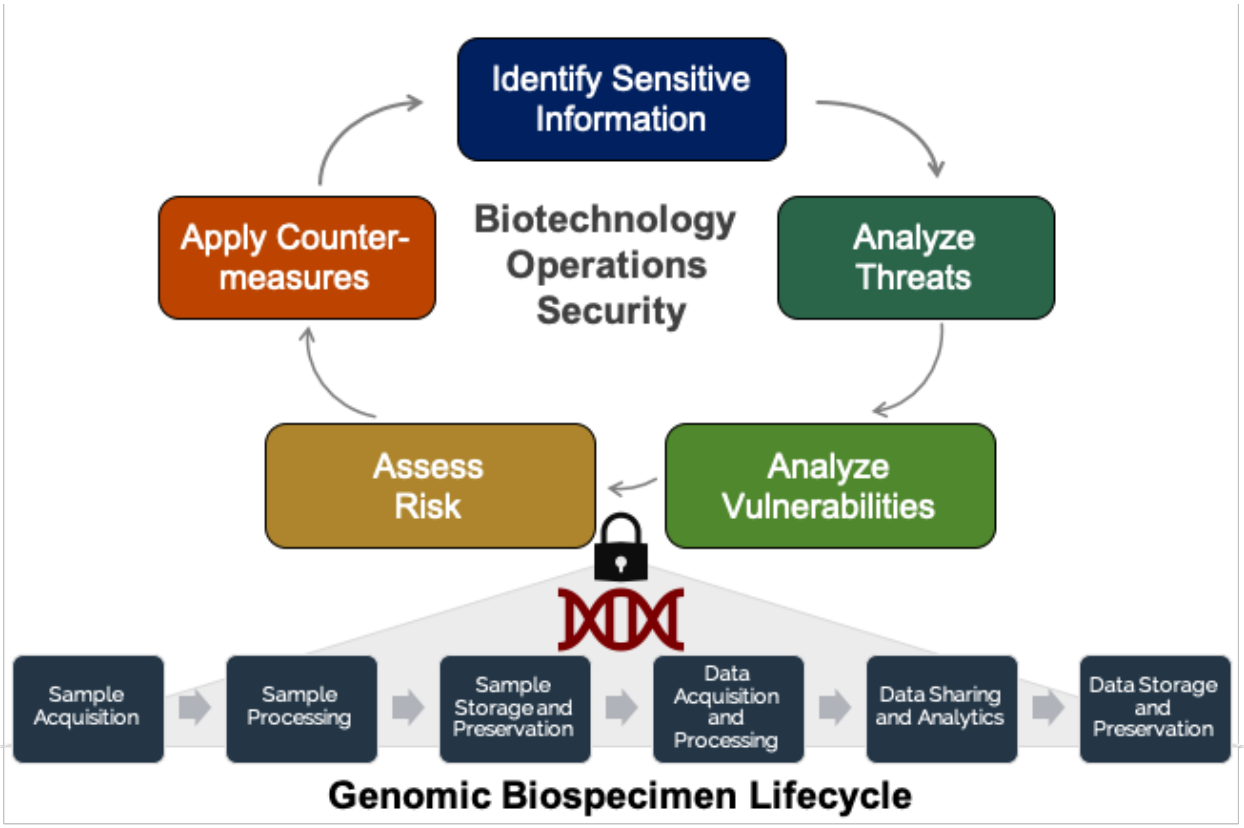

Figure 2: Biotechnology Operations Security (BioOPSEC) Milestones. Throughout the lifecycle of genomic samples and data, it is critical to ensure sample and data integrity. Major milestones of BioOPSEC are: 1) Identification of Sensitive Information, 2) Analysis of Threats, 3) Analysis of Vulnerabilities, 4) Assessment of Risk, and 5) Application of Countermeasures. BioOPSEC can be applied by any institutions involved in biological data procurement, storage, and use. By including consideration of adversary capabilities and domain-specific security considerations, BioOPSEC is not limited to a finite set of rule-based compliance measures. By reducing barriers for operator collaboration (such as expertise siloes and use of jargon), BioOPSEC encourages participation and responsibility by any operator involved in data integrity and privacy. The BioOPSEC framework can readily be exchanged with a corporate, trade-secret emphasis to extend across the full range of bioeconomy operations.

To demonstrate the BioOPSEC process, we describe the chain of custody of a genomic biospecimen throughout its lifecycle in a simulated multi-site precision medicine study. Our contribution here is to outline an adversary-conscious approach that can motivate multiple technical communities. As the BioOPSEC approach is agnostic of data type, environment, and operator skillset, it is our hope that it is broadly adopted across the biotechnology enterprise.

3.0 METHODS

We sought to establish a balanced, multidimensional systems analysis process that could be applied by both military and civilian institutions involved in biomedical data procurement, storage, and use. First, we conducted a comprehensive analysis of current legislative requirements for biomedical data security, real-world biomedical research workflows, and likelihood of novel attacks against biomedical data. In order to solicit subject matter expertise and collaboration from scientific and security researchers, we organized the first Federal Precision Medicine Technical Exchange, which was attended by precision medicine and security leaders from federal agencies including the DoD, VA, NIH, and FBI. We analyzed best practices for supporting friendly operations within the DoD as well as with allied nations. To examine novel security vulnerabilities, we reviewed relevant federal, state, and military-specific legislation that may provide guidance on data security and privacy rules, including HIPAA, FISMA, and FIRRMA. To evaluate feasibility of security and privacy attacks, we reviewed biological, artificial intelligence, and cybersecurity literature. We integrate this knowledge into the existing DoD Operations Security (OPSEC) framework so that it is tailored for use with biomedical data and optimizes opportunities within the DoD biotechnology community. To test our BioOPSEC framework, we simulate a precision medicine multi-site research study in a military laboratory wherein we trace chain of custody for a genomic sample, highlight sensitive information, and analyze security gaps, threats, vulnerabilities, and risks. We demonstrate how to prioritize application of countermeasures throughout the biospecimen lifecycle. Using a systems approach, we propose overarching recommendations to support implementation of standardized, multi-layered security procedures suitable for disparate environments.

4.0 RESULTS AND DISCUSSION

4.1 BioOPSEC in Context: Precision Medicine Research and Risks to an Operational Environment

Using the example of executing a multi-site precision medicine research study with secondary use, we systematically apply BioOPSEC principles to each of the study processes. Depending on study design, size, and extent of multi-institution collaboration, we consider that sample and data processes for research genomics could occur at disparate sites and executed by different operators (**Figure 3**). For each step in the genomic biospecimen lifecycle, we identify vulnerabilities, assess risk while exploring countermeasures and value optimization. This process can also be applied to private sector scenarios where preservation of intellectual capital is a concern.

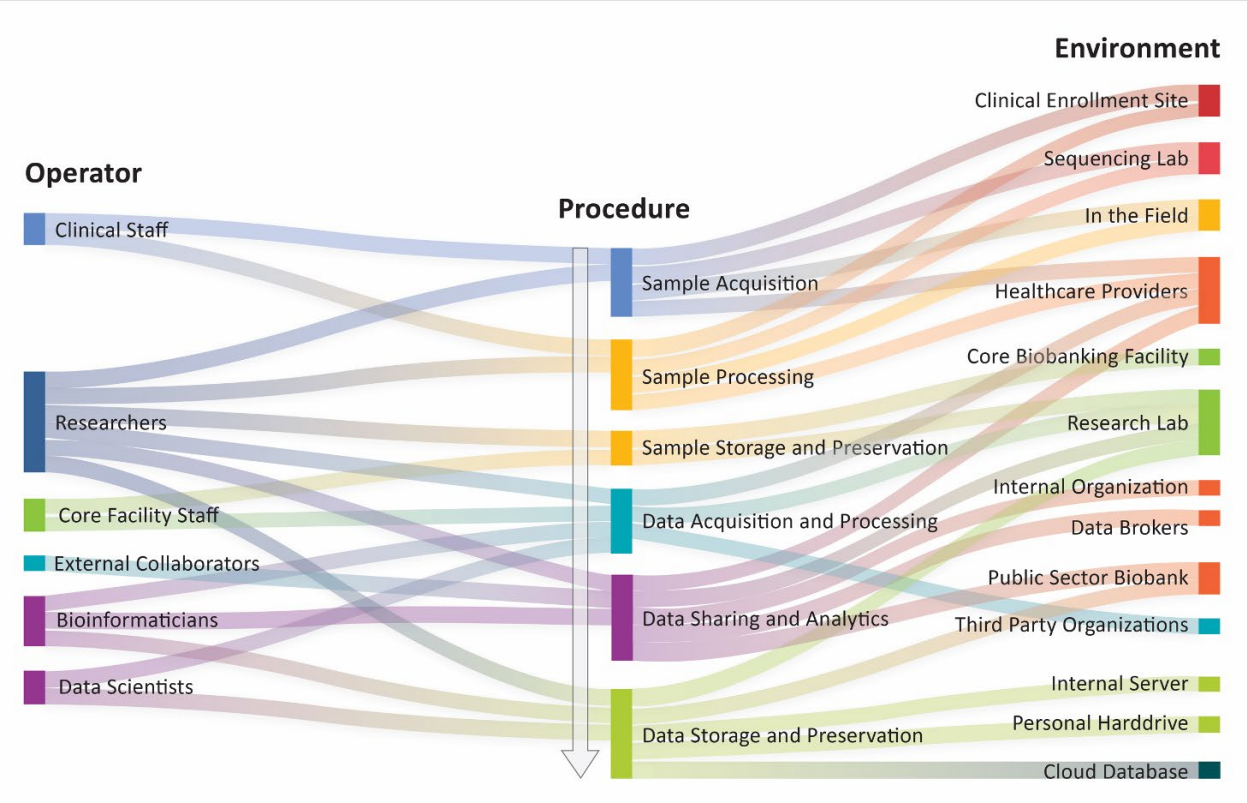

Figure 3: Representative Chain of Custody in the Genomic Biospecimen Lifecycle. Many operators work together in multiple and diverse environments to achieve each step in the lifecycle of a genomic sample. Additionally, if the sample acquisition site is different than that of either the sample processing or storage sites, the sample may travel through an intermediate courier. As data become extracted from genomic samples, the likelihood of duplication of either raw or modified data grows. This amplification represents significant challenges to robust data validity, lineage tracing, and responsible stewardship.

4.2 Sample Acquisition, Processing, Storage and Preservation.

Vulnerabilities: Genomic samples are vulnerable to theft, destruction, mishandling, and tampering throughout the procurement process. A multitude of processing steps can result in mislabeling, mishandling and/or inappropriate storage of samples.[17], [18] Exploitation of these vulnerabilities can occur via insider, physical, and supply chain attacks. An insider threat is a prototypic vulnerability that can originate from operators within any of the organizations

orchestrating sample procurement or their trusted business partners who is negligent, ignorant, compromised, or criminal. This vulnerability exists throughout the chain of custody.

Countermeasures: Personnel reliability programs (PRP) can be implemented to increase operator trust and encourage a culture of ownership and advocacy. Both the military and civilian organizations have standards for personnel reliability that enable continuous process improvement (e.g., ISO9001:2015). Robust inventory control measures can help mitigate the risks of sample theft, destruction, mislabeling and/or mishandling. For example, creation and storage of audit trails to track sample access history, sample verification methods to assure data quality[19], [20], and process tracking to assure the integrity of the sample data.[21] Multi-layered access control should be instituted throughout the environment. Security responsibility, such as periodic monitoring of samples, should be performed. A second, non-redundant sample storage location may be considered, likely with the archived sample under more stringent access control. Where possible, rich metadata should be catalogued in a secure and standardized fashion.

4.3 Data Acquisition and Processing

Vulnerabilities: Raw sequencing files can be procured at disparate sites by different operators and have inconsistent formats (**Figure 3**). Different choices of parameters and bioinformatics pipelines, particularly during variant annotation, contribute to variability[22], threatening data integrity and long-term value. Emergent risks include sophisticated supply chain and side-channel attacks, such as reconstruction of a DNA sequence using a microphone positioned near the DNA synthesizer.[23]

Countermeasures: Specific countermeasures include physical security around the sequencing equipment and an information technology approval process that tests the security of the equipment before it begins operation (e.g., "authority to operate" within the Federal Risk and Authorization Management Program). Standardized meta-data, version control techniques, and carefully selecting open source tools[1] (e.g., BioCompute Objects, Apache Atlas, Pachyderm) can also play important roles in risk mitigation.

4.4 Data Sharing and Analytics

Vulnerabilities: Data sharing and analytics frequently involve electronic transfer of data across organizational boundaries and can therefore be the source of multiple vulnerabilities in the pipeline, including disclosure (accidental or intentional), interception, and widespread distribution and/or duplication. Each organization (research labs, healthcare providers, public sector biobanks, international organizations, data brokers, etc.) will likely have different policies on handling data, especially if the organizations are across jurisdictional boundaries. Haphazard data lineage tracing – a process to highlight where copies of the data are stored and how they have been modified – is a critical concern.

Countermeasures: Maintaining a ground-truth copy of the data is important. Technologies such as cloud (where data use does not require duplication) or blockchain (where a distributed ledger identifies data provenance) may help to mitigate these risks. A data management plan outlining data architectures and sharing methods would make withdrawal of consent (or dynamic consent) possible, especially when system interoperability and governance are emphasized during development. Emerging techniques such as privacy preserving data-mining methods can also protect data security and privacy while optimizing utilization.[24]

4.5 Data Storage and Preservation

Vulnerabilities: Data duplication in different locations (Figure 3) creates different thresholds of responsible data stewardship of the preserved and newly analyzed versions of the data. As long-term storage of genomic data is vulnerable to theft, destruction and manipulation (Table 1), a primary risk is the compromise of the data integrity, especially if data are not properly curated with standardized metadata and responsible stewardship.

Countermeasures: Ongoing curation of genetic and genomic data is critical to empowering data findability, accessibility, interoperability, and re-usability. Techniques such as exome reinterpretation as new variants are discovered can ensure ongoing utility, while low cost storage in an appropriately secured cloud environment can facilitate preservation.

	Identify Sensitive Information	Analyze Threats	Analyze Vulnerabilities	Assess Risks	Apply Countermeasures
Sample Acquisition	--Storage location --De-identified label encoding	--Insider attacks --Physical attacks	--Theft --Destruction --Mishandling --Tampering	**Low**	--Stringent access control (locks, swipe cards) --Audit trails --Sample verification methods
Sample Processing	--Software parameters for variant annotation	+Supply chain attacks	+High degree of analysis variability	**Low-mid**	--In-depth log file to track software parameters
Sample Storage	--Storage conditions --Labeling	+Non-state actors	+Loss	**Mid**	--Periodic auditing of samples
Data Acquisition and Processing	--Informed consent attributes --De-identification mechanisms for data	+Cyber attacks	+Interception +Disclosure (accidental or intentional)	**Mid**	--Robust and integrated informed consent procedures
Data Sharing and Analytics	--Record of sharing (data lineage) --Sensitive data set or model parameters	+Interception attacks	--Widespread distribution and/or duplication	**High**	--Responsible data stewardship --Mechanisms for data lineage tracing --Machine learning defense techniques

Data Storage and Preservation	--Locations, procedures, and documentation of storage mechanisms --Archival and redundancy details	+State competitors +Near peer adversaries	+Theft +Destruction +Loss of data	**High**	--Detailed curation of data and metadata

Table 1: Application of BioOPSEC Across the Biospecimen Chain of Custody. As data is extracted from genomic samples, the amount of sensitive information markedly expands. As a result, the types of exploitable vulnerabilities and potential threats also grow (denoted by plus sign). This exercise highlights that countermeasures should be prioritized to secure and protect data sharing, analytics, and storage. Importantly, we examine potential vulnerabilities within these procedures and highlight applicable countermeasures, including physical, personnel, administrative, and technological controls.

5.0 CONCLUSION AND RECOMMENDATIONS

Ultimately, the rapidly evolving biotechnology landscape requires deep technical expertise and adaptive capabilities to achieve optimal development and mitigate risk. Here we have presented BioOPSEC, an extensible framework for proactive identification of vulnerabilities, threat modeling, and prioritized deployment of countermeasures. BioOPSEC can be broadly applied across the biotechnology research enterprise by organizations in friendly or adversarial contexts. Additionally, it is agnostic of data type, environment, and operator expertise. By driving intellectual convergence and encouraging high ownership of security by personnel, the BioOPSEC framework empowers implementation of standardized, multi-layered security procedures in disparate environments and operators. Adoption of these procedures could help to efficiently safeguard biomedical data, optimize operational tradeoffs, accelerate data sharing through increased technical interoperability, and protect participant privacy in support of the bioeconomy.

As part of BioOPSEC, we propose three overarching recommendations for adoption within the biotechnology research enterprise for a systems-level view.

Motivate institutional engagement and ownership of security. In order to encourage participation, facilities should convene the necessary stakeholders in a working group similar to those described in DoD OPSEC guidelines.[25] Such a working group could be composed of subject matter experts in information technology, infrastructure, and security; clinical health care and research; bioinformatics; and data science.[1] Facilities can conduct periodic incident response drills to identify gaps in the response procedures, ensure experiential learning among their operators, and address continuous process improvement. Hands-on security training may also be beneficial.

Encourage intellectual convergence and exchange. Opportunities for knowledge exchange and collaboration could include collaborative events such as institution-specific research symposia, seminars, online or hands-on training, etc. Ethical hacking and red teaming are foundational principles in cybersecurity for testing systems, tools, and policies to identify security weaknesses. Exchanging the latest best practices[1] ensures defenses are keeping up with emergent threats throughout a multi-layered network of collaborators.

Enable centralized control and decentralized execution. Another principle of BioOPSEC is to add decentralized responsibility for maintaining security. Individual operators need training to underscore the importance of upholding security: for example, that these data come from people, and the linkage of different datasets can unexpectedly impact the lives of those people.[26] A method to objectively evaluate the benefits of continuous training is also important for continuous improvement.[27]

6.0 References

[1] E. National Academies of Sciences and Medicine, *Safeguarding the Bioeconomy*. Washington, DC: The National Academies Press, 2020.

[2] J. Shendure, G. M. Findlay, and M. W. Snyder, "Genomic Medicine-Progress, Pitfalls, and Promise," *Cell*, vol. 177, no. 1, pp. 45–57, Mar. 2019, doi: 10.1016/j.cell.2019.02.003.

[3] K. E. Boronow *et al.*, "Privacy Risks of Sharing Data from Environmental Health Studies.," *Environ Health Perspect*, vol. 128, no. 1, p. 17008, Jan. 2020, doi: 10.1289/EHP4817.

[4] M. D. Edge and G. Coop, "Attacks on genetic privacy via uploads to genealogical databases," *bioRxiv*, p. 798272, Jan. 2019, doi: 10.1101/798272.

[5] Y. Erlich, T. Shor, S. Carmi, and I. Pe'er, "Re-identification of genomic data using long range familial searches," *bioRxiv*, p. 350231, Jan. 2018, doi: 10.1101/350231.

[6] M. Naveed *et al.*, "Privacy in the Genomic Era," *ACM Comput Surv*, vol. 48, no. 1, Sep. 2015, doi: 10.1145/2767007.

[7] P. G. Consortium *et al.*, "Public access to genome-wide data: five views on balancing research with privacy and protection," *PLoS Genet*, vol. 5, no. 10, p. e1000665, Oct. 2009, doi: 10.1371/journal.pgen.1000665.

[8] R. M. Hendricks-Sturrup and C. Y. Lu, "Direct-to-Consumer Genetic Testing Data Privacy: Key Concerns and Recommendations Based on Consumer Perspectives," *J Pers Med*, vol. 9, no. 2, May 2019, doi: 10.3390/jpm9020025.

[9] W. N. 2nd Price and I. G. Cohen, "Privacy in the age of medical big data.," *Nat Med*, vol. 25, no. 1, pp. 37–43, Jan. 2019, doi: 10.1038/s41591-018-0272-7.

[10] "S. 2098 — 115th Congress: Foreign Investment Risk. Review Modernization Act of 2018." 2018.

[11] Jackson, James., "The Committee on Foreign Investment in the United States (CFIUS)." Congressional Research Service., Aug. 06, 2019, Accessed: Aug. 27, 2019. [Online]. Available: https://fas.org/sgp/crs/natsec/RL33388.pdf.

[12] R. E. Clifford, D. Baker, V. B. Risbrough, M. Huang, and K. A. Yurgil, "Impact of TBI, PTSD, and Hearing Loss on Tinnitus Progression in a US Marine Cohort," *Mil Med*, Feb. 2019, doi: 10.1093/milmed/usz016.

[13] M. K. Taylor, L. M. Hernández, M. R. Schoenherr, and E. J. Stump, "Genetic, Physiologic, and Behavioral Predictors of Cardiorespiratory Fitness in Specialized Military Men," *Military Medicine*, 2019, doi: 10.1093/milmed/usz033.

[14] N. A. Kimbrel, M. E. Garrett, M. F. Dennis, M. A. Hauser, A. E. Ashley-Koch, and J. C. Beckham, "A genome-wide association study of suicide attempts and suicidal ideation in U.S. military veterans," *Psychiatry Research*, vol. 269, pp. 64–69, Nov. 2018, doi: 10.1016/j.psychres.2018.07.017.

[15] A. J. Titus, E. van Opstal, and M. Rozo, "Biotechnology in Defense of Economic and National Security.," *Health Secur*, vol. 18, no. 4, pp. 310–312, Aug. 2020, doi: 10.1089/hs.2020.0007.

[16] Department of Defense, "Joint Publication 3-13.3. Operations Security." Jan. 04, 2012, Accessed: Sep. 09, 2019. [Online].

[17] C. PERROW, *Normal Accidents*, REV-Revised. Princeton University Press, 1999.

[18] FDA. Director of Laboratory Science and Safety, “FDA Review of the 2014 Discovery of Vials Labeled ‘Variola’ and Other Vials Discovered in an FDA-Occupied Building on the NIH Campus,” *Report to the Commissioner*, Dec. 2016.
[19] “Biobanking: How the Lack of a Coherent Policy Allowed the Veterans Administration to Destroy an Irreplaceable Collection of Legionella Samples,” *Hearing Before the Subcommittee on Investigations and Oversight, Committee on Science and Technology. House of Representatives.*, vol. 110th Congress, 2008.
[20] C. Pellerin *et al.*, “A Simple Variable Number of Tandem Repeat-Based Genotyping Strategy for the Detection of Handling Errors and Validation of Sample Identity in Biobanks,” *Biopreserv Biobank.*, no. 1947-5543 (Electronic), 2016.
[21] K. A.-O. http orcid org Zych *et al.*, “reGenotyper: Detecting mislabeled samples in genetic data,” *PLoS One*, no. 1932-6203 (Electronic), 2017.
[22] J. Vaught, “Biobanking Comes of Age: The Transition to Biospecimen Science,” *Annual Review of Pharmacology and Toxicology*, vol. 56, no. 1, pp. 211–228, Jan. 2016, doi: 10.1146/annurev-pharmtox-010715-103246.
[23] S. Roy *et al.*, “Standards and Guidelines for Validating Next-Generation Sequencing Bioinformatics Pipelines: A Joint Recommendation of the Association for Molecular Pathology and the College of American Pathologists,” *J Mol Diagn*, vol. 20, no. 1, pp. 4–27, Jan. 2018, doi: 10.1016/j.jmoldx.2017.11.003.
[24] S. Faezi *et al.*, “Oligo-Snoop: A Non-Invasive Side Channel Attack Against DNA Synthesis Machines,” presented at the Proceedings 2019 Network and Distributed System Security Symposium, 2019, doi: 10.14722/ndss.2019.23544.
[25] A. Mohammed Yakubu and Y.-P. P. Chen, “Ensuring privacy and security of genomic data and functionalities,” *Briefings in Bioinformatics*, no. bbz013, Feb. 2019, doi: 10.1093/bib/bbz013.
[26] Department of Defense, “Operations Security Program Manual,” 2008, [Online]. Available: https://fas.org/irp/doddir/dod/m5205_02.pdf.
[27] M. Zook *et al.*, “Ten simple rules for responsible big data research,” *PLoS Comput Biol*, vol. 13, no. 3, p. e1005399, Mar. 2017, doi: 10.1371/journal.pcbi.1005399.
[28] D. Talwar, T. S. Tseng, M. Foster, L. Xu, and L. S. Chen, “Genetics/genomics education for nongenetic health professionals: a systematic literature review,” *Genet Med*, vol. 19, no. 7, pp. 725–732, Jul. 2017, doi: 10.1038/gim.2016.156.