GOING VIRAL: BIOECONOMY DEFENSE

2023 TABLETOP EXERCISE

JOHNS HOPKINS APPLIED PHYSICS LABORATORY

bioisac

2023

LESSONS LEARNED REPORT

Jeremy Ratcliff, PhD[1]

F. Connor Sage, ME[1]

Brian Haberman, PhD[1]

Sophia Oluic, MPH[1]

Whitney Bowman-Zatzkin, MPA, MSR[2]

Charles Frick, MS[1,2]

Charles Fracchia, MS[2]

[1]The Johns Hopkins University
Applied Physics Laboratory
11100 Johns Hopkins Rd.
Laurel, Maryland 20723-6099

[2] The Bioeconomy Sharing and Analysis Center
(BIO-ISAC)

CONTENTS

EXECUTIVE SUMMARY

In May 2023, the Johns Hopkins University Applied Physics Laboratory, together with the Bioeconomy Information Sharing and Analysis Center, hosted a two-day tabletop exercise to expand participant awareness of the complexities inherent to the bioeconomy when facing a cybersecurity incident. Several dozen individuals with expertise across public health, policy, cyber, physical sciences, and law were brought together to identify vulnerabilities, develop mitigation recommendations, and establish a greater understanding of the extent of the threats that currently exist in key biological capabilities through participating in a fictional scenario. Ultimately, this effort identified four key areas for action:

TRUST — AWARENESS — RESPONSIBILITY — PREPAREDNESS

Trust between a researcher and their research equipment is necessary to make informed decisions regarding a research question; additionally, trust is required between a manufacturer and a regulatory body to ensure that produced goods and services are safe and effective for their intended use. The public, reliant on products developed by the bioeconomy, trust that the collaborations between researchers, manufacturers, and regulators are robust enough to protect their interests. The bioeconomy depends on assumed integrity of adjacent actions; when just one piece is corroded, the whole system becomes compromised.

Despite the equivalency between laboratory instrumentation and traditional information processing and storage equipment, there is a gap between regulatory awareness of biological practices and cybersecurity digital security practices. Among all entities of the bioeconomy ecosystem there is insufficient exposure to (1) best practices for safeguarding and (2) digital vulnerabilities facing the bioeconomy.

The existing structures within the United States Government (USG) and private sector are not well poised to handle cross-domain issues, such as digital security threats against laboratory instruments and processes at the world's testing, research, and manufacturing sites. Roles and responsibilities within the bioeconomy ecosystem are undefined for most aspects of preparedness and response to digital security threats.

Achieving preparedness to detect, mitigate, and remediate threats to the bioeconomy will require a process that is amenable to change and flexible to support the expansion of new research thrusts. Digital security vulnerabilities are increasingly pervasive in the bioeconomy, but responsible agencies and industry partners lack sufficient guidance, policy, and structure to respond rapidly and effectively.

To address articulated needs in each of these action areas, recommendations include strengthened intra-agency coordination, data life cycle documentation, education and training, process workflow creation and assessment, and the creation of guidance documents that standardize industry-wide digital security practices and principles specific to the bioeconomy's needs. Implementing these recommendations will help ensure a safer and more secure bioeconomy that can continue to create new services and products for the benefit of the United States of America and the world.

EVENT BACKGROUND

In May 2023, the Johns Hopkins University Applied Physics Laboratory (APL), through its partnership with the Bioeconomy Information Sharing and Analysis Center (BIO-ISAC), hosted a tabletop exercise (TTX) to test the resiliency of the bioeconomy through a scenario illustrating the potential impact of cybersecurity threats. Several dozen individuals from across the public health, policy, cyber, physical sciences, biotechnology, and law domains participated in the two-day exercise. This document summarizes the structure of the exercise and takeaways gathered from participant input.

The bioeconomy is a critical component of the present and future United States economy and national security. As defined by the Congressional Research Service, the bioeconomy is "the share of the economy based on products, services, and processes derived from biological resources."[1] It is composed of a complex network of biomedical, bioindustrial, and agricultural domains, and currently accounts for five to seven percent of the United States Gross Domestic Product according to the National Academies report *Safeguarding the Bioeconomy*.[2] The pace of innovation in the bioeconomy is accelerating as new tools and technologies become available to industry and academic partners. These innovations include continued refinement of emerging laboratory techniques such as CRISPR (clustered regularly interspaced short palindromic repeats) and single-cell sequencing; ever increasing use of artificial intelligence and machine learning (AI/ML) in the biological sciences; and expanding access to and scalability of cloud-based solutions for data management, analysis, and even laboratory capacity.[3] Some industry estimates project the value of the global bioeconomy will grow from $1 trillion to nearly $30 trillion United States dollars (USD) over the next two decades.[4] In September 2022, the Biden administration launched a National Biotechnology and Biomanufacturing Initiative via Executive Order 14081.[5] Subsequent reports led by the President's Council of Advisors on Science and Technology and the White House Office of Science and Technology Policy have affirmed the role of this sector to the future of the United States economy and national security.[6,7]

As the digital transformation becomes more embedded in the bioeconomy, so do the digital security risks facing the sector. While these threats are not unique to the bioeconomy, risks are increased by the presence of technologies and resources vulnerable to cyber intrusions, the high potential for inexperience in the cybersecurity domain amongst those establishing bioeconomy-related startups, and the value of intellectual property (IP) held by these companies. Further, as highlighted in *Safeguarding the Bioeconomy*, the reliance on large datasets and databases, open-source software, and internet-based exchange of data increase risks for this sector specifically.[2] Recent high-profile attacks, such as the Tardigrade threat beginning in 2020, data breaches at Dr. Reddy's Laboratories, and the EvoTec ransomware attack,[8–10] have helped bring these vulnerabilities and threats to the attention of the industry, regulators, and policymakers.

While much of Executive Order 14081 focuses on initiatives and programs to accelerate growth of the bioeconomy (i.e., a bio-based procurement policy and expanding training and education opportunities), two sections fully or partly focus on methods to address these digital vulnerabilities. Section 5 (d) (i) directs the Department of Homeland Security

to assess the cyber and physical vulnerabilities of the bioeconomy; make recommendations to secure those vulnerabilities; and enhance coordination with industry on threat information sharing, vulnerability disclosure, and risk mitigation. Section 8 calls for a multi-agency review of the regulatory landscape for biotechnology and specifies roles, responsibilities, and gaps in regulatory authority.

Safeguarding the bioeconomy is an economic necessity and urgent national priority. The response to the COVID-19 national emergency relied upon effective, timely, and trusted data and information. These information flows were shown to be vulnerable at most steps of the data life cycle, from generation to inclusion in informational products. The domestic rise of misinformation is an exemplar of this effect; leveraging the extraordinary amount of data being generated about the novel pathogen, malicious actors capitalized on confusing and sometimes conflicting information to push a narrative to benefit their self-interests.[11] Nefarious actions at this intersection of the digital and biology realms can threaten the United States' economic competitiveness and national security, impede the deployment of medical responses, undermine perceived safety of response actions, and significantly degrade processes necessary for response development. These vulnerabilities in our bioeconomy can be abused, as adversaries and strategic competitors use legal and illegal means to acquire United States technologies and data, including biological data and proprietary or pre-competitive information.[12]

In 2021, the BIO-ISAC was chartered to serve as a resource for digital threat detection, prevention, protection, response, recovery, and resilience within the bioeconomy. ISACs have served as hubs for cyber threat detection and reporting across domains to protect critical infrastructure in the United States since Presidential Decision Directive 63 in 1998.[13] One of the core roles the BIO-ISAC serves is to be the central resource for gathering information on digital threats impacting the bioeconomy infrastructure and for two-way communication of this information between and among the public and private sectors. BIO-ISAC products include detailed reports on identified cyberattacks, a curated list of real-time disclosed cyber threats, threat hunting services, and industry recommendations and guidance for safe and secure operations, workforce development, and training.

EXERCISE

1. EXERCISE STRUCTURE

The bioeconomy defense exercise was an unclassified, in-person event that took place on May 16 and 17, 2023, at APL's campus in Laurel, MD. Participants were identified and recruited to the event based on several factors: (1) participant expertise and experience, (2) participant department/organization, (3) participant attendance at a previous bioeconomy workshop in January 2023, and (4) the participants' displayed interest in the subject matter. Once registered, participants were assigned to a discussion group in advance of the event to distribute subject matter expertise between groups. The exercise was hosted under TLP:CLEAR[a] and a modified Chatham House rule.[b]

The exercise consisted of a fictional scenario presented chronologically through six vignettes spread evenly over both days. After the vignette was presented, artifacts were distributed to all discussion groups. These artifacts included fictional social media posts, news releases, press statements, and other material that supplemented the new information made available at the opening of each new vignette. Participants then broke out into their pre-assigned discussion groups and were instructed to summarize their reactions and the immediate remediation steps they would propose, which were captured by notetakers. In the event of a pause in conversation, moderators had a list of pre-prepared questions for each vignette to redirect participants toward topics of interest to the event organizers. Approximately halfway through each vignette, new information was injected through presentation and additional fictional artifacts. Often, this information introduced or progressed side narratives, several of which were designed to distract or confuse participants. At the end of each vignette and respective inject, participants reconvened to present main findings, concerns, and decision points from each discussion group. This helped broaden participants' knowledge and perspectives on how other members of the bioeconomy would respond to the scenario vignettes.

The event was led by four main moderators, and each group was staffed with one moderator and one or more notetakers. All moderators and notetakers were briefed on and had access to the complete event narrative. During the discussion portions of the exercise, lead moderators moved around the room to answer questions, encourage discussions, and help groups proceed past sticking points.

[a] The Traffic Light Protocol (TLP) is a set of designations to protect sensitive information outside the remit of the collateral classification protocol. For more details, please see: https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage.

[b] There would be no attribution of information or quotes to individuals or organizations, but a list of exercise participant affiliations may be included in publications following the event.

While participants were able to submit requests for information, their actions and decision making did not impact the narrative. There were instructions to consider the appropriate response by government officials, but participant-proposed actions were not evaluated against a set of objectives. Rather, participants were instructed to reflect on the reliability and relative importance of (sometimes conflicting) information and to articulate what actions they would take if they were in a position of responsibility during the response.

2. OVERVIEW OF EXERCISE NARRATIVE AND RESPONSES

The following completely fictional storyline was created for the scenario of the event. The narrative was constructed to highlight the complex challenges associated with identifying, characterizing, and responding to digital threats. Revealed over the course of the exercise, participants had to reckon with hacking, leaking of confidential information, manipulation of databases, misinformation campaigns, and potentially compromised laboratory equipment.

The bioeconomy defense exercise placed participants at the center of decision making during the response to a growing domestic outbreak of Nipah virus, a highly pathogenic infectious disease for which there are no licensed medical therapeutics or vaccines. Several months prior to the first vignette where participants entered the scenario, the USG declared the outbreak a public health emergency due to the widespread seeding of cases across the United States, the high risk for establishment as an endemic pathogen in wild boar populations, and the lack of available medical countermeasures.

Perceiving the outbreak as a potential means for diversifying their income beyond their traditional market of second- and third-line tuberculosis antibiotics, Vivalife Therapeutics (VVL) licensed an experimental vaccine from an academic partner that had, years prior, successfully completed a phase I trial before failing to find external funding. At the start of the event, VVL completed a successful nationwide phase II/III trial for their vaccine and received an emergency use authorization (EUA) from the Food and Drug Administration (FDA).

2.1 VIGNETTE 1: RISING PUBLIC NARRATIVE APPEARS

Narrative Overview

Within a few days of the vaccine receiving its EUA, a rising public narrative gains traction on social media. The theory states that the recently approved vaccine specifically causes damage to the respiratory system of Hispanic people. There is no data in the public domain that supports the narrative, and there are significant inconsistencies in messaging among those promoting the public narrative. Several scientists use their personal social media accounts to challenge the public narrative and are invited guests on mainstream news networks. Still, the number of people sharing the narrative steadily increases. The narrative does little to stem the flow of vaccines into arms, however, and nearly three and a half-million individuals receive a dose of the vaccine by the end of the second week of the vaccination campaign.

After a few weeks, a social media journalist widely known for “debunking” medical misinformation posts a long-form article on their blog, reporting that many accounts amplifying the public narrative are suspicious: they have short account histories, few followers, nondescript usernames, and appear to be posting identical or near-identical messages without clear links between the accounts (e.g., they are not following each other).

Participant Responses

From the onset of group discussions, it was clear that COVID-19 altered the threat landscape regarding the circulation of mis-, dis-, and malinformation online, especially in public messaging and engagement from federal entities. Participants mentioned that the time and manner in which the public is engaged is crucial for understanding the threat and shaping the response. They suggested a focused and coordinated messaging campaign between the federal government, local government, and private sector. At this point in the event, some groups had minor concerns that the public narrative could be fueled by a malicious actor, but no actions were recommended to assess this risk.

2.2 VIGNETTE 2: PUBLIC DATA DISCLOSURE

Narrative Overview

Documents emerge on BitTorrent (a decentralized, peer-to-peer file sharing protocol) claiming to contain raw data from VVL's EUA submission. These documents purportedly reveal raw data that supports the notion that individuals of Hispanic ethnicity faced a much higher likelihood of experiencing a serious adverse event (SAE) following vaccine administration. Crucially, the application dossier submitted to the FDA's Vaccines and Related Biological Products Advisory Committee (VRBPAC) did not include this data. Independent media outlets and personal social media accounts swiftly embrace the leaked documents as credible, amplifying the narrative in their engagements with the public. Even major cable news networks are discussing the contents, albeit with emphasis that the documents are unverified. Concurrently, reports of individuals experiencing respiratory distress after vaccine uptake proliferate on social media. These accounts are accompanied by screenshots of submissions to the Vaccine Adverse Event Reporting System (VAERS) co-managed by the FDA and Centers for Disease Control and Prevention (CDC). However, public health researchers and clinicians take to local media and individual social media channels to clarify the intricacies of VAERS reporting, citing the absence of supporting evidence from the clinical reporting portal, although noting those reports can be further delayed in time.

The inject moved participants to six weeks into the vaccine campaign, where ten million individuals have been vaccinated to date, but the rate of vaccination is tailing off. The landscape further evolves when the BIO-ISAC publishes a vulnerability in a commercial DNA sequencing technology in coordination with the National Institute of Standards and Technology (NIST) Computer Security Incident Response Team (CSIRT). The vulnerability includes the means to remotely alter raw sequencing output. Almost immediately, several prominent news outlets report that the vulnerable sequencing technology is the same model as that listed within VVL's EUA submission. This revelation is entangled with the original narrative, VAERS reporting, and BitTorrent leaks, setting in motion a new and fast-moving narrative on social media. At vignette closing, VVL has released no public statements nor held any press conferences.

Participant Responses

Prior to the inject, participants across multiple groups expressed distrust in the authenticity of the leaked documents. The individuals that viewed the documents as legitimate questioned the route through which they entered the public domain and suggested the FDA take punitive actions against VVL for failing to submit all the trial data. Some individuals believed that the documents were leaked by an insider threat — potentially motivated by insider trading or ethical duty. Nearly all participants acknowledged that verification of document authenticity would almost certainly require VVL's input because third-party verification would be challenging and time-consuming. Further, it was unclear which federal entity would manage third-party verification. Once the DNA sequencer vulnerability was introduced, many participants changed their position. Recommended responses were severe, with a sizable number of individuals across groups calling for immediate cessation of vaccine administration pending an independent investigation. Participants criticized the lack of communication from VVL.

2.3 VIGNETTE 3: PAUSE IN VACCINE ADMINISTRATION

Narrative Overview

The FDA announces the extraordinary action of pausing vaccine administration, stopping people from receiving the vaccine, pending an investigation of both the data submission and the increase in VAERS reporting. Following the FDA announcement, VVL provides their first public comments. In a press conference, VVL announces they are investigating their internal data in concert with Apex Clinical Research, a contract research organization (CRO) that collaborated with VVL during the phase II/III trial of the vaccine. The press conference provides no information on the origin or authenticity of the trial documents posted on BitTorrent. Shortly after the press conference, a new cadre of documents appear online, this time containing copies of internal VVL emails. These demonstrate VVL researchers raising concerns to senior leadership about the data not being present in the EUA submission. An author of one of the emails takes to their personal social media to deny the email legitimacy, but later corrects himself and states that VVL legal counsel has advised him the email had been located in the company email server.

After the press conference, an action group called Families Advocating for Critical Thinking (FACT) is launched via a blitz of reporting on independent media. In a press conference, FACT mentions the compromised DNA sequencer and formally accuses VVL of having knowledge of the vulnerability and its capacity to compromise data from the DNA sequencer during the clinical trial for the vaccine. FACT leadership is invited on several prominent podcasts where they call for an investigation into VVL.

Participant Responses

The pause in vaccine administration challenged the participants. Many individuals commented that the agency placed themselves in a position where future actions would inherently appear political. Several participants noted they were not sure how the government could reinstate trust in the vaccine or the vaccine approval process. Despite these issues, many participants vocalized agreement in pausing administration. When asked: "*What do you believe was the tipping point for the FDA pausing vaccine administration*?", most groups pointed to BIO-ISAC's announcement of the DNA sequencer vulnerability, despite no evidence of a direct connection between the vulnerability announcement and VVL's specific machines being provided.

2.4 VIGNETTE 4: INTERNAL AND EXTERNAL INVESTIGATIONS

Narrative Overview

The pause in vaccine administration results in turmoil within VVL. The company's stock falls significantly, and many employees go on the record that they are leaving due to concerns about the company's leadership and integrity. Within this period of uncertainty, a portion of a confidential presentation from the CEO to investors is leaked online. The presentation contains numerous significant reports: repeated analyses of internal trial data support the documents published on BitTorrent; these new findings are inconsistent with reports received from the CRO at the end of trial; and the DNA sequencer vulnerability has been remediated but it's uncertain what impact it has had on company products.

Once the presentation has been leaked, VVL goes on the defensive. VVL hosts another press conference where they announce that they are hiring a third-party cyber forensics company to perform an investigation into the discrepancy between the new analysis and the reports received from the CRO. FACT, who has steadily gained national prominence, hosts a press conference where they dismiss VVL as peddling fake news and announce that they have received a new $5 million donation to their campaign.

Participant Responses

At this stage, participants started growing frustrated with VVL's response. Still, individuals noted that, despite a lack of confidence in VVL, the government was inherently reliant on their vaccine as no vaccine alternatives had been introduced. Groups diverged in their views about the most pertinent issues. Some groups viewed VVL as transparent, while others treated them with suspicion. One group focused on the discrepancy between the data held by VVL, the CRO, and the FDA. They questioned adherence to the data use agreements signed between VVL and the CRO. Toward the end, several groups focused their discussions on cybersecurity and spent time trying to resolve how to balance regulation and incentives to motivate better cybersecurity standards in the bioeconomy.

2.5 VIGNETTE 5: ESCALATION TO CRIMINAL INVESTIGATION

Narrative Overview

In a joint statement, VVL and the FDA announce that interim results of the third-party cyber forensic investigation point toward intrusions into VVL's information technology systems. The case has been referred to the Federal Bureau of Investigation (FBI) for independent assessment and verification. Separately, the FDA and CDC jointly announce that an internal investigation into the uptick of reporting in VAERS has failed to verify many of the severe reports submitted by the public reporting route. Simply, most reports do not have matching records at medical facilities and certain patient metadata in the forms appears to be randomly generated. Lastly, investigative journalists uncover evidence of physical cash transfers between the leaders of FACT and an agent of a foreign power. FACT denounces the investigation but notably ceases making public appearances or statements.

Participant Responses

At this point, almost all groups recognized that VVL had been a victim of a cyberattack and that the vaccine was safe and efficacious. One group, however, remained bearish against VVL because of the DNA sequencer vulnerability and did not believe that the announcement of the FBI investigation should absolve VVL of responsibility. Other groups viewed the invitation of the FBI as a strong indication of VVL's innocence; one participant criticized the response for not inviting the FBI into the investigation earlier given the seriousness of the situation.

Groups noted that it would be a substantial task to regain public trust in the vaccine. Despite the original trial conclusions upon which the EUA was granted being legitimate, the persistent news coverage and uncertainty around the vaccine presented an extraordinary challenge. One group believed that the dichotomous options available to the response were to either maintain public trust in the vaccine approval process or promote VVL's vaccine, but not both.

2.6 VIGNETTE 6: INVESTIGATION CONCLUDES

Overview

The FBI's report corroborates the assessment of the third-party cyber forensics company. There was a significant breach of VVL's IT systems. Upon entry, the hackers were able to modify existing databases and email servers and extract pre-competitive information and internal documentation. The FDA ends the pause in administration and individuals begin receiving doses again, but at a much slower rate than prior to the documents appearing on BitTorrent. VVL's board removes the current CEO and replaces them with an individual who promises to increase the company's cybersecurity standards. BIO-ISAC publishes a threat assessment and after-action report that includes a list of recommendations to secure cyber systems at biomanufacturing sites, including best practices in hardware and software acquisition and processes for sunsetting equipment.

As the final inject, a foreign company announces that their vaccine, which is based on the same vector as VVL's, has surpassed efficacy and safety expectations two months after the FBI report. This company is suspected, but not confirmed, to have ties with a nation's investment infrastructure. This same nation announces that they had pre-purchased hundreds of millions of doses of the vaccine and that they will be offering discounted doses to select regions of the world.

Participant Responses

Prior to the inject, most groups took this vignette as an opportunity to vocalize their overall impressions from the exercise. Many individuals stated that there should be extended regulation in place to ensure the security of laboratory devices but were unsure what would be the appropriate level of regulation to not disadvantage the companies on the global market. Similarly, individuals were not able to identify which federal agency would or should have jurisdiction over this regulation, and who would be responsible for investigating potential adherence lapses. Individuals were frustrated about the lack of security at VVL, with one participant commenting that "*all these things happened because one private company didn't have the right security.*"

HIGH-LEVEL TAKEAWAYS

The bioeconomy is crucial to the growth and protection of the nation. This is increasingly evident by the USG's continued focus on the growth and preeminence of US-based biotechnology, including biomanufacturing.[2,6,7] In addition to the economic benefits that a growing bioeconomy will bring, there is ample potential for misuse of or nefarious intent related to developed technologies and products. Effective strategies to protect the bioeconomy and ensure its proliferation must be implemented.

The bioeconomy is vulnerable to digital threats. Stakeholders must be made aware of these risks, and solutions must be acted upon at all levels, from technical professionals through policymakers. The bioeconomy is composed of multiple sectors, which complicates the implementation of these solutions. It was evident from the TTX that the USG is underprepared to adequately regulate and efficiently govern the bioeconomy of the near future. Further, industry stakeholders are uninformed about the threats they face and ill-equipped to detect or mitigate active digital threats.

The participants of the TTX were thrust into a scenario that revealed concerning gaps in the United States' ability to respond to threats within the bioeconomy. From the participant responses, four action areas were identified, outlining improvements for increased effectiveness in identifying, mitigating, and recovering from cyber-based threats to the bioeconomy: Trust, Awareness, Responsibility, and Preparedness.

3. TRUST

The bioeconomy produces goods and services, like vaccines and therapeutics, that are critical to national security, public health, and public safety. These goods and services rely strongly on information science, data analysis, and AI/ML as a component of the life sciences research process. The 2020 National Academies report on *Safeguarding the Bioeconomy* identified three common features of information systems across the bioeconomy:[2] (1) the bioeconomy relies on large databases, often of commercially or personally sensitive information; (2) some components of the bioeconomy rely on open-source software packages, often of uncertain quality, robustness, and degree of maintenance; and (3) the bioeconomy relies on internet communications to exchange data (e.g., publicly available genome data). This data-rich environment necessitates trust between the researcher and the research equipment in order to make informed decisions regarding a research question; additionally, it necessitates trust between a manufacturer and a regulatory body to ensure the goods and services are safe and effective for the intended use.

Corruption within the biotechnology information pipeline poses a significant risk to the success of the bioeconomy. The recently revised (October 2022) *National Biodefense Strategy and Implementation Plan* dictates that "evidence-driven, coordinated response operations and investigations" are required to rapidly respond to a bioincident.[14] In this context, the phrase 'evidence-driven' implies the use of biotechnology (e.g., a DNA sequencer) to resolve an investigation. Distortion of that evidence could result in missteps in response. There is implicit trust then in the researcher's judgement of data generated by a piece of research equipment and analyzed by a software tool or online database, while both equipment and software may have vulnerabilities unrecognized or unknown to the researcher. The opportunities for this system to be compromised are extensive, while the researcher's ability to evaluate the fidelity of the data is limited.

The bioeconomy depends on assumed integrity of adjacent actions; when just one piece is corroded, the whole system becomes compromised.

3.1 TRUST — FINDINGS

Throughout the exercise, several participants noted the importance of trustworthy data. Several common themes were identified.

1. Trust in lab equipment performance and data handling is foundational to the bioeconomy. Reestablishing or remediating trust is not straightforward. Event participants had difficulty proposing or identifying evaluation and testing methods to reestablish and verify data integrity.
2. Authenticity of data matters. Each step in the data life cycle, from raw observation on an instrument to inclusion in policy, involves generating, manipulating, and transmitting data between parties. Malfeasance at any step will impact each stage downstream of the incident. As the number of parties involved in the chain of custody for data increases, the challenge of establishing the provenance of a cyber incident increases significantly.

Notable Quotations:

- "[It is] impossible to know what to trust."
- "If [the sequencer] was compromised, then we need to stop the vaccine because we can't confirm it was safe."

3.2 TRUST — RECOMMENDATIONS

To address concerns stemming from the potential to lose trust in the information systems within the bioeconomy, several recommended actions were identified.

1. The USG should develop, and eventually expand, digital security standards for laboratory equipment, especially those in areas of research or industry that are critical to the nation's proliferation, protection, and growth (e.g., biotechnology and biomanufacturing).
2. As there are potential vulnerabilities at each step in the data life cycle, preparedness for and mitigation of threats must consider each waypoint. Hardening waypoints along the path of data generation and use will lessen the propagation of adversarial actions, as will establishing best practices for tracking and indicating data provenance.
3. Introducing a system with tiered levels of compliance, similar to the structure of physical security or biological safety, will facilitate participation across the spectrum of research and industry partners.

In addition to the recommendations outlined above, Recommendation 6 of the *Safeguarding the Bioeconomy* report should be recognized for its relevance:

"All bioeconomy stakeholders should adopt best practices for securing information systems (including those storing information, intellectual property, private-proprietary information, and public and private databases) from digital intrusion, exfiltration, or manipulation."[2]

4. AWARENESS

Life sciences researchers are not typically trained to engage with digital security policy as it relates to best practices in the laboratory. Research equipment generates, collects, and analyzes data, often while connected to a network. Networked laboratory equipment is equally or more vulnerable to network threats as any laptop or printer. Even indirectly connected equipment often uses data from a networked node, transferred by removable media, to perform its function. Many of the traditional cybersecurity threats also pose great risk to biotechnology. In spite of the equivalency between laboratory instrumentation and traditional information processing and storage equipment, there is a void between regulatory awareness of biological practices and digital security practices. Further, equipment within the bioeconomy is infrequently recognized as part of a digital infrastructure.

Resulting from a lack of collective awareness, sensitive and specific portions of the bioeconomy, such as -omics datasets, personally identifiable information (PII), protected health information (PHI), or intellectual property (IP), are vulnerable to tampering and misuse.[2] At an industrial scale, biomanufacturing facilities may be equally vulnerable to threats posed against industrial process control systems. In either scenario, the outcome of poorly protected equipment will be damaging to the research or industrial body and will increase potential for harm to the nation's people, animals, agriculture, and environment.

The BIO-ISAC serves as the central resource for gathering information on digital biosecurity threats and for two-way communication of this information between and among the public and private sectors. The chartering of the BIO-ISAC indicates progress toward growing digital biosecurity awareness and best practices within the bioeconomy, but it is underutilized and not well known by the communities most in need.

Among all entities of the bioeconomy ecosystem there is insufficient exposure to (1) best practices for safeguarding and (2) vulnerabilities against the bioeconomy.

4.1 AWARENESS — FINDINGS

Throughout the event, participants regularly noted both their concern over laboratory-based cyber vulnerabilities and their lack of familiarity with appropriate remediation steps. They did not know how to act upon these concerns confidently, leading to confusion and frustration in their response to the challenge.

1. Event participants from both the private and public sector were largely unaware of cyber vulnerabilities facing the bioeconomy and the steps needed to protect against and respond to a cybersecurity event. This applied to both lab equipment (e.g., DNA sequencers) and support systems (e.g., email servers).
2. Many event participants were unfamiliar with the BIO-ISAC and how it could be leveraged in the event scenario.

Notable Quotations:

- Participant to BIO-ISAC: "Door is open. Please, how fast can I get you?"
- "We need to get the word out there on BIO-ISAC … [to create] awareness that it exists for pharmaceutical industry."

4.2 AWARENESS — RECOMMENDATIONS

To increase opportunities for raising awareness, several recommended actions were identified.

1. Additional exercises that enhance digital coordination across USG agencies represented in the bioeconomy ecosystem should be hosted regularly, and results should be disseminated broadly.
2. BIO-ISAC should expand efforts with private sector and state and federal agencies, highlighting its capacities, abilities, services, and resourcing as a trusted member of the community.
3. Slick sheets, advertising campaigns, and incentive programs could be used to increase the collective awareness of threats.

5. RESPONSIBILITY

Our bioeconomy is comprised of a broad collection of technical disciplines, with significant growth expected to occur year over year. Within this rapidly expanding ecosystem, novel biotechnology products will be created, and new fields will emerge. As the use of and reliance on the bioeconomy increases, so too will challenges stemming from the diversity, complexity, and sophistication of the products and manufacturing processes.[6] Exceeding global competition and meeting the demand signal of these goods and services will require a well-organized infrastructure, whose entities' roles are clearly defined by an equally organized regulatory body.

A first step toward defining roles and responsibilities is clear communication. Transparency in communications with and data sharing by domestic and international partners is vital for success.[14] The existing structure within the USG and private sector is not well poised to handle cross-domain issues, such as digital security threats against laboratory equipment. The report on *Biomanufacturing to Advance the Bioeconomy* highlighted the complexity of the problem:

> "However, many new bioproducts do not align with a single regulatory process entry point or pathway. Therefore, bioproducts may not fit neatly within agency jurisdictions under existing statutes, and the framework does not have guidance to help companies determine which agency or agencies have jurisdiction over their product or components of their product."[6]

If there will be challenges in bringing goods to the market, then it should also be expected that responses to digital security incidents afflicting the bioeconomy will be lagging, insufficient, ineffective, or inefficient due to systemic decision-making paralysis or duplicative efforts. It is crucial then to identify organizations that are well-equipped to engage in policymaking, or to define new roles for existing organizations where necessary. Implementation of digital security standards will also require elucidation. It is imperative to clearly define the responsibilities that will fall on the device or software manufacturer versus the equipment user, and to balance potentially detrimental impacts while doing so (e.g., loss of profit, reduced production throughput, and reputational risk).

Roles and responsibilities within the bioeconomy ecosystem are undefined for most aspects of preparedness and response to digital security threats.

5.1 RESPONSIBILITY — FINDINGS

Participants of varying backgrounds found difficulty in identifying roles and responsibilities within the USG and industry, stifling their ability to mitigate threats throughout the exercise.

1. Responsibility for ensuring digital integrity of biological devices, at the national level, was unclear. Participants highlighted the fine line between establishing standards and the risk of over-regulation.
2. While most authorities are in place across government agencies, the responsibility for acting against threats to the bioeconomy is either assumed to be handled or passed along from one agency to the other with little to no coordination.

Notable Quotations:

- “Clearer guidance about who has enforcement authority related to bioeconomy issues would be helpful. For example, there are clear enforcement standards and actions for HIPAA-related violations."
- "How do you motivate companies to pursue tighter cybersecurity on these devices?"

5.2 RESPONSIBILITY — RECOMMENDATIONS

Recommendations were prepared for how to delegate responsibility prior to, during, and after a cybersecurity threat to the bioeconomy.

1. The USG should draft a process workflow for identifying cybersecurity vulnerabilities and indicators of attacks, complete with clearly defined roles and discrete delineations between responsible parties and for use cases relevant to the bioeconomy.
2. New inter-agency groups may be required, bringing added capabilities to existing organizations.
3. Strive for action in unison. Increased collaboration between public and private sectors would enable rapid and effective communications and reporting of cybersecurity breaches, anticipated vulnerabilities, or recommended improvements—akin to Consumer Product Safety Commission recalls.
4. Approaches to tighten cybersecurity on laboratory devices need to balance incentives and enforcement when considering new regulation.
5. Define and deploy a shared responsibility model for equipment that leverage cloud-based services with clear delineation of responsibility between the original equipment manufacturer and asset owner.

6. PREPAREDNESS

With roles clearly defined, awareness of the threat space effectively communicated, and trust soundly established with the information systems, bioeconomy stakeholders will be well poised to defend against potential threats. However, there must be an emphasis on the fluidity of changes to the bioeconomy and the rapid rate at which new complexities may be added. Increasing data generation, adoption of new and transformative technologies, and potential for nefarious use are contributing factors to the growing complexity of the bioeconomy.

There is a need to maintain national preeminence in the growth and development of the global bioeconomy, but the adoption of best practices to fortify the bioeconomy will be resource intensive and will require effective and rapid communication between governing bodies. A system that is amenable to change and flexible to support the expansion of new research thrusts is required to be truly prepared for threat detection, mitigation, and remediation.

In support of an amenable and flexible support system, stakeholders in the bioeconomy will need to develop, exercise, and update risk mitigation and communication plans with regularity. Risk assessment must be a cornerstone of operations in the growing bioeconomy, and the risks must be respected and well understood by all parties.

Digital security vulnerabilities are increasingly pervasive in the bioeconomy, but responsible agencies and industry partners lack guidance, policy, and structure to respond rapidly and effectively.

6.1 PREPAREDNESS — FINDINGS

The exercise pressed the limits of the participants' traditional threat mitigation strategies, pushing them into unfamiliar positions and stifling their ability to request help.

1. Event participants from several domains, including health, were responsible for a significant portion of the pandemic response but were unable to identify appropriate remediation steps after the cyber threat was revealed.
2. Due to the lack of messaging and coordination between agencies, knowledge sharing is extremely limited, resulting in a lack of cross-domain preparedness. Agencies are then asked to fund projects and programs to address traditional bioeconomy threats without the depth of understanding of the cyber ecosystem.

Notable Quotations:

- "This is too big a problem for me to solve. I need help."
- "Nobody [in our domain] is really prepared for advanced cyberattacks."

6.2 PREPAREDNESS — RECOMMENDATIONS

1. The USG should perform, with the cooperation of private industry, iterative assessments of critical infrastructure and/or critical functions (physical and digital) within the bioeconomy to ensure its enduring resiliency.
2. To anticipate the necessary response to a complex and evolving threat, cross-domain training should be provided to officials with the bioeconomy ecosystem. Primarily, health and digital security domain collaboration must increase.
3. Policies and procedures should be established for an inter-agency group to rapidly respond to a digital biosecurity threat in a private industry partner that has brought a laboratory instrument or countermeasure to market.

ADDITIONAL TAKEAWAYS

7. GAPS IN VULNERABILITY PERCEPTION

In vignette two of the training exercise, the BIO-ISAC, in coordination with the NIST CSIRT, released a public report on a vulnerability in a commercial sequencing technology. The commercial DNA sequencer happened to be the same model as was reported in VVL's submission for an EUA, and public narratives spread online that the DNA sequencer vulnerability, VAERS reports, and BitTorrent leaks were all interrelated. This proved to be the most significant inject within the exercise. Nearly every group viewed the DNA sequencer vulnerability as a major factor behind the FDA's pause of the EUA and, later in the exercise, viewed it as justification to keep the EUA paused.

However, the DNA sequencer vulnerability was a red herring. At no point in the exercise was it confirmed or even hinted by authoritative sources that the vaccine stock was adulterated. While some individuals recognized that the vulnerability in isolation was not significant (see quote below), the conclusions reached within each group overwhelmingly overemphasized the DNA sequencer vulnerability and its role within the FDA's decision making. Further, several groups viewed the DNA sequencer vulnerability as an indication of incompetence on the part of VVL. While the exercise was intentionally structured to cast doubt on the reliability of VVL, the condemnation of VVL for the (lack of) security of commercial-off-the-shelf (COTS) equipment used in their processes was unexpected.

> "We have to remember; it is the sequencer model but not this [specific] instrument that was compromised."

This inject was inspired by the critical vulnerabilities announced for Illumina sequencing systems in April 2023.[15] In this way, this inject was one of the most realistic scenarios presented to participants during the exercise and thus makes analysis of the response more pertinent. The antagonistic response to VVL from many of the participants raises several important areas for discussion. Resolving these questions was not the aim of the exercise. The following areas should be prioritized in future discussions within the community:

- What is the appropriate distribution of responsibility when laboratory equipment is shown to be vulnerable? Potential parties include the equipment manufacturer, the company purchasing and using the equipment, risk management and site insurers, and regulatory agencies.
- Many entities within the bioeconomy rely on open-source and licensed software for their business processes. What are reasonable expectations for private companies to perform independent vulnerability assessment for open-source and COTS software and equipment?
- How should regulatory agencies respond if equipment used in a process that has received an EUA or full licensure is shown to have vulnerabilities? What processes should a regulatory agency have in place to characterize or determine cyber vulnerabilities? Which entity carries responsibility for end-user safety, harm, and risk?

Lastly, one group raised concerns with the timing of the vulnerability announcement by the BIO-ISAC. That group believed BIO-ISAC was either taking advantage of the situation to raise their profile or failing to recognize the impact of the vulnerability announcement on VVL's viability. As stated on its website (isac.bio/disclosure) and aligned with industry best practices for coordinated disclosure, BIO-ISAC "facilitates ethical disclosure of any vulnerability" and "requires that stakeholder(s) be given time to assess and fix vulnerabilities before public disclosure." BIO-ISAC should continue efforts to coordinate announcements with potentially impacted private companies and must maintain its independence to provide this support.

8. RELEVANCE OF GEOGRAPHIC ORIGIN OF CYBERATTACK

Throughout the event, there was no clear indication made to participants as to the country of origin of the social media misinformation campaign, disclosure of privileged information, or cyber intrusion into VVL's systems. There was some evidence that the political action group FACT was wholly or partially being financed by a foreign government, but it was intentionally made clear to the participants that this was not directly linked to the cyber vulnerabilities. As noted by many participants, the inability to confirm the provenance of the attack limited the entities that could be involved in the response. Namely, no capabilities, competencies, or knowledge from the Department of Defense or some organizations within the Intelligence Community could legally be leveraged until the cyberattack was confirmed to be carried out by individuals not on United States soil. Even prior to the cyberattack being revealed, event participants were lamenting the inability to leverage certain government assets during the apparent social engineering campaign in the first vignette. Some event participants affiliated with these organizations felt sidelined even though they believed their internal capabilities would benefit the group. Responses to real threats may be hamstrung if there are significant delays in identifying the geographic origin of a cyberattack.

Cyber attribution, as a technical domain, is challenging. As argued by Rid and Buchanan (2015), the process is more art than science and is dependent on technical, human, and political factors that can confound clear-cut conclusions.[16] Navigating these intricacies in a timeframe that is relevant to response activities necessitates developing and refining attribution methodologies. By expanding the boundaries of cyber forensic capabilities, we can not only enhance our ability to attribute cyberattacks but perhaps anticipate and counteract future threats more effectively.

There are further challenges with pursuing cyber attribution due to its divergent importance between private and public entities. For stakeholders in industry, determining the origin of an attack is far less valuable than responding to the immediate impact of the threat on business operations. For government, attribution is key for mobilizing certain assets. Motivating industry to both disclose experienced threats and pursue cyber attribution in the wake of an event are significant hurdles. These challenges are an opportunity for organizations such as the Cybersecurity and Infrastructure Security Agency (CISA), FBI, and BIO-ISAC to offer assistance in performing attribution and for cybersecurity developers to continue to expand the tools and capabilities available to teams conducting cyber attribution.

9. CHALLENGES WITH SHORING UP CAPABILITIES FOR SMALL COMPANIES

In the exercise, VVL was presented as a large, established company that has previously brought pharmaceutical products to market. Participants could assume that the company was sufficiently well-resourced to have information technology departments and staff with some expertise in cybersecurity. In conversations toward the conclusion of the event, many participants noted that the scenario would have played out significantly different had VVL been a smaller company. In those instances, VVL would be far less likely to have internal capabilities to handle or even recognize a cyber intrusion and may have simply ceased operations as a company.

Like other domains, a portion of the bioeconomy consists of smaller companies and startups. These companies are at significantly higher risk of cyber intrusions, as previously highlighted in *Safeguarding the Bioeconomy*.[2] These companies simply lack the resources or experience to fend off attackers. Particularly in a challenging and competitive economic environment, small companies are even less likely to allocate their budgets to cybersecurity which may, much to their peril, be perceived as having lower priority when compared to investments in product and business development. BIO-ISAC supports membership pathways for new businesses in the industry, offering reduced rates for early-stage companies and pathways to membership through investors and collaboratives. Expanding participation and increasing awareness of these options should be an industry-wide priority.

This gap presents as an opportunity space for an organization such as BIO-ISAC to offer services to these companies to facilitate a robust and secure bioeconomy. These actions could be as nonspecific as the dissemination of best practice tactics, techniques, and procedures (TTPs) to improve digital security or as tailored as threat hunting and disclosure of identified vulnerabilities.

CONCLUSION

This bioeconomy defense exercise prompted participants to manage the consequences of a cyber intrusion of a critically important company during the response to a health crisis. The manipulations of the cyber threat, rooted in historical events, authentically exposed vulnerabilities within the bioeconomy. Participants were challenged to respond to the information made available to them, and generally failed to recognize the cyberattack prior to the reveal in vignette five. This event demonstrated that a similar scenario, played out in the real world, could have lasting and damaging impacts on the bioeconomy.

Insights derived from the exercise highlight four priority areas for additional policy and technical development: Trust, Awareness, Responsibility, and Preparedness. The exercise centered on compromised trust between a private company, a regulatory body, and the public. Recommendations to fortify trust largely rely on USG and include enhanced digital security standards and tiered compliance levels. The exercise also demonstrated insufficient awareness of cyber threats among members of the bioeconomy. Convening additional exercises inviting a wider network of bioeconomy stakeholders is one means of increasing awareness of this challenge amongst the community. Participants had trouble identifying which agencies had responsibility over specific aspects of the response; clarifying these roles would increase the efficiency and effectiveness of future responses. Lastly, many participants were quick to admit that they felt unprepared to appropriately respond to the scenario presented to them. Cross-domain training for officials that may be involved in future responses should be prioritized.

Discussions between participants also yielded additional minor takeaways. These include the clear need for regulatory guidance for laboratory equipment used in the development of medical countermeasures, emphasis on the importance of identifying the geographic origin of a cyberattack, and recognition of the challenge in ensuring small companies are prepared for cyber threats. The latter, in particular, is an opportunity for an organization such as the BIO-ISAC to have a significant role in increasing the cyber resiliency of the bioeconomy.

With the United States bioeconomy poised for global influence, enhancing its capacity to detect and counter digital threats is paramount. Strengthening the bioeconomy's resilience ensures the continued provision of its existing products and services and ability to continue to be a world leader in innovation, benefiting both the nation and the global community.

REFERENCES

1. Gallo M. The bioeconomy: a primer. R46881 Congr Res Serv. 2021.

2. National Academies of Sciences and Engineering. Safeguarding the bioeconomy. National Academies Press; 2020.

3. Lentzos F, Ivernizzi C. Laboratories in the cloud. Bulletin of the Atomic Scientists. 2019 . Available from: https://thebulletin.org/2019/07/laboratories-in-the-cloud/

4. Cumbers J. Forbes. White House Unveils Strategy To Grow Trillion Dollar U.S. Bioeconomy. Available from: https://www.forbes.com/sites/johncumbers/2022/09/12/white-house-inks-strategy-to-grow-trillion-dollar-us-bioeconomy/

5. Executive Order 14081. 88 FR (25711-25715) Sep 15, 2022. Available from: https://www.federalregister.gov/documents/2022/09/15/2022-20167/advancing-biotechnology-and-biomanufacturing-innovation-for-a-sustainable-safe-and-secure-american

6. President's Council on Advisors of Science and Technology. Biomanufacturing to Advance the Bioeconomy. Executive Office of the President; 2022 Dec. Available from: https://www.whitehouse.gov/wp-content/uploads/2022/12/PCAST_Biomanufacturing-Report_Dec2022.pdf

7. White House. Building the Bioworkforce of the Future. 2023 Jun. Available from: https://www.whitehouse.gov/wp-content/uploads/2023/06/Building-the-Bioworkforce-of-the-Future.pdf

8. BIO-ISAC. BIO-ISAC. 2021. Threat Advisory - Tardigrade: an APT attack on vaccine manufacturing infrastructure. Available from: https://www.isac.bio/post/tardigrade

9. Stupp C. WSJ. Biotech CEO Gets Hands-On After Cyberattack to Protect Business. Available from: https://www.wsj.com/articles/biotech-ceo-gets-hands-on-after-cyberattack-to-protect-business-9c6d08fe

10. Liu A. Dr. Reddy's shuts "key" plants worldwide after potential cyberattack hits COVID work | Fierce Pharma. 2020. Available from: https://www.fiercepharma.com/pharma-asia/dr-reddy-s-hit-by-cyber-attack-amid-russian-covid-19-vaccine-work

11. van der Linden S. Misinformation: susceptibility, spread, and interventions to immunize the public. Nat Med. 2022 Mar;28(3):460–7.

12. Sabbagh D. Hackers "try to steal Covid vaccine secrets in intellectual property war." The Guardian. 2020 Nov 22; Available from: https://www.theguardian.com/world/2020/nov/22/hackers-try-to-steal-covid-vaccine-secrets-in-intellectual-property-war

13. United States: National Archives and Records Administration: Office of the Federal Register. Presidential Decision Directive 63 on Critical Infrastructure Protection. Fed Regist Vol 63 No 150. 1998 Aug 5;41707–955.

14. White House. National Biodefense Strategy and Implementation Plan. 2022 Aug. Available from: https://www.whitehouse.gov/wp-content/uploads/2022/10/National-Biodefense-Strategy-and-Implementation-Plan-Final.pdf

15. Herper M. FDA warns of security vulnerability in Illumina's DNA sequencing machines. STAT. 2023. Available from: https://www.statnews.com/2023/04/27/fda-warns-vulnerability-illumina-sequencing-m/

16. Rid T, Buchanan B. Attributing Cyber Attacks. J Strateg Stud. 2015 Jan 2;38(1–2):4–37.

APPENDIX A. ACRONYMS

AI	Artificial Intelligence
APL	Johns Hopkins University Applied Physics Laboratory
BIO-ISAC	The Bioeconomy Information Sharing and Analysis Center
CDC	Centers for Disease Control and Prevention
CISA	Cybersecurity and Infrastructure Security Agency
COTS	Commercial-off-the-shelf
CRISPR	Clustered Regularly Interspaced Short Palindromic Repeats
CRO	Contract Research Organization
CSIRT	Computer Security Incident Response Team
EUA	Emergency Use Authorization
FACT	Families Advocating for Critical Thinking
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
IP	Intellectual Property
ISAC	Information Sharing and Analysis Center
ML	Machine Learning
NIST	National Institute of Standards and Technology
PHI	Personal Health Information
PII	Personally Identifiable Information
SAE	Serious Adverse Event
TLP	Traffic Light Protocol
TTPs	Tactics, Techniques, and Procedures
TTX	Tabletop Exercise
USD	United States Dollar
USG	United States Government
VAERS	Vaccine Adverse Event Reporting System
VRBPAC	Vaccines and Related Biological Products Advisory Committee
VVL	Vivalife Therapeutics