Prepared Testimony of Matthew F. McKnight - General Manager, Ginkgo Biosecurity
Before the House Energy & Commerce Committee
Subcommittee on Oversight and Investigations
Hearing on "Examining Biosecurity at the Intersection of AI and Biology"
December 17, 2025

1-page Summary:

- **Biology is the New Strategic Domain:** Biology will define the next era of security and geopolitics, much like chemistry, physics, and computing defined the 20th century. While adversaries are rapidly operationalizing biotechnology as a strategic asset, the United States and its allies remain unprepared for the threats to come from this development.

- **Failure of International Institutions:** Traditional biosecurity frameworks, specifically the World Health Organization (WHO) and the Biological Weapons Convention (BWC), have failed to provide necessary transparency or enforcement. These types of multilateral agreements and international cooperation are critical, but without scaled and independent technical verification, these institutions have been unable to compel rapid sample sharing or verify lab incidents, leaving the U.S. vulnerable to adversaries who exploit these gaps through secrecy.

- **The Shift to BIOINT (Biological Intelligence):** The solution to these failures is technical, not political. The U.S. must build "BIOINT," a real-time technical collection-focused intelligence system (akin to SIGINT, MASINT, etc.) capable of detecting, analyzing, and attributing biological threats immediately. This shifts the focus from relying on diplomatic goodwill to generating hard technical intelligence that enables this cooperation.

- **Building Biothreat Radar:** To generate this intelligence, the U.S. must deploy "Biothreat Radar," a global, persistent sensor grid that turns the planet into a living detection network. This system continuously monitors nodes such as airports, border crossings, farms, municipal wastewater plants, laboratories, and other strategic sites to identify genomic anomalies in real time through modalities such as wastewater, air, and surface swabs.

- **Attribution Creates Deterrence:** A key objective of BIOINT is contributing to attribution—the ability to forensically prove the origin of a biological event. Establishing that bad actors cannot hide their actions creates an immediate strategic cost, providing the same deterrence logic that has governed nuclear security for decades.

- **Establishing a New Industrial Base:** The U.S. needs a dedicated biosecurity industrial base that operates in both peacetime and wartime modes. In peacetime, this industry acts as a detection engine; in wartime, it flips to rapid response, manufacturing countermeasures like vaccines within days rather than months.

Prepared Testimony of Matthew F. McKnight - General Manager, Ginkgo Biosecurity
Before the House Energy & Commerce Committee
Subcommittee on Oversight and Investigations
Hearing on "Examining Biosecurity at the Intersection of AI and Biology"
December 17, 2025

Chairman Joyce, Ranking Member Clarke, Chairman Guthrie, Ranking Member Pallone, and Members of the Subcommittee:

Thank you for the opportunity to testify before the Committee. My name is Matthew McKnight, and I am the General Manager of Ginkgo Biosecurity, the biosecurity technology-focused subsidiary of Ginkgo Bioworks (NYSE: $DNA). We are a U.S.-based company building technology-forward global biosecurity infrastructure (biothreat radar) to help governments and organizations detect, analyze, and respond to biological threats, whether naturally occurring or man-made; thereby transforming environmental samples into high-fidelity data assets.

Our work is predicated on the belief that biology will define the next era of security and prosperity. While our strategic rivals rapidly operationalize biotechnology as a strategic domain, America and our allies remain unprepared for the threats to come. We lack unified and scaled modern biosecurity infrastructure capable of detecting, deterring, and neutralizing biological threats before they destabilize militaries, economies, or societies. We must build this technological backbone of biosecurity to enable timely and effective response.

This Iron Curtain of Biology divides our world. On one side, dangerous regimes conduct clandestine research behind walls of secrecy, and refuse to share data on outbreaks that threaten the world. On the other, America and its allies have yet to build robust detection systems that respect individual rights while securing our collective future. If we do not act, we risk losing our advantage to adversaries who view biology not just as science—but as strategic leverage.

A Strategic Crossroads

We stand at a definitive crossroads regarding our biological security. Two scenarios—both plausible—paint starkly different futures for the United States and its allies.

1. The Biological Event Ending the American Century

The following scenario is not difficult to imagine: a decade from now, a fast-moving respiratory virus erupts in Southeast Asia, killing 4-6% of those infected, mostly children and young adults. Yet again, U.S. and WHO surveillance falter and the pathogen spreads globally before its severity is fully understood by authorities. Though the origins of the virus aren't clear, Beijing, after decades of biotech investment, unveils a 90 percent-effective vaccine clearly developed before the first public cases and trades doses for strategic concessions. Washington must queue behind China's partners and accept unfavorable terms while deaths mount and markets crater.

In Washington, there is outrage but no real choice. Lack of preparedness and an inability to independently produce and manufacture countermeasures has led to a full-blown national crisis. Overnight, the center of geopolitical gravity tilts east, proving that whoever controls biology, and biosecurity, controls the balance of power.

Questions are asked: How did America not know about China's vaccine development program, or the risky gain of function research that was (perhaps) linked to it? Why weren't we prepared to respond? But the intelligence failure doesn't matter, it's too late.

2. Allied Biosecurity and Shared Prosperity

At this same crossroads, an alternate scenario is also plausible: By 2035, the U.S. and its allies operate Biothreat Radar, a global sensor grid and biological intelligence (BIOINT) cloud that turns bio-signals into real-time threat intelligence. Tamper-proof DNA synthesis

audits and pervasive monitoring make clandestine engineering nearly impossible. Nations that decline membership still live under the network's optics. Cross-border air sampling, satellite-linked monitors on air transit, and biosensors at ports ensure compliance even beyond alliance borders.

When a novel avian flu appears in a member state, it's rapidly sequenced and flagged. BIOINT confirms its natural origin and auto-generates vaccine designs. Distributed manufacturing across allied biofoundries initiates production almost immediately, containing the outbreak before travel disruptions take hold. The global public remains calm.

This swift, coordinated response reflects a decade of investment in secure data sharing, distributed production, and harmonized regulation. The same infrastructure that deters risky research and defends against biothreats now also powers a new era of bio-abundance—tailored vaccines, sustainable crops, and economic resilience, shared across the alliance.

One future is characterized by dependence, instability and defeat. The other, sovereignty, resilience, and leadership.

The Stakes: What History Tells Us

History teaches that every transformative technology—chemistry, physics, computing—has revolutionized warfare, the economy, and geopolitics.

- **1910s - Chemistry in WWI:** Chemistry revolutionized the 20th century, turning oil into everyday products like plastics and fertilizers. It also shaped World War I with the introduction of chemical weapons such as mustard gas, chlorine, and mass-produced high explosives, forever changing the nature of modern warfare. Despite their devastating impact, prohibitions on chemical weapons came too late for their victims.

- **1930s-1940s - Physics in WWII:** Humanity's ability to understand and apply physics has eventually allowed us to access the stars and enabled humanity's increasing connectivity. In the 1930s and 1940s, it also brought about aerial warfare, the need for radar, and the nuclear age. The atomic bombings of Hiroshima and Nagasaki demonstrated the unprecedented destructive power of weaponized physics, creating a new existential threat.
- **1950s-1980s - Computing in the Cold War and War on Terror:** The advent of the computer chip is the backbone for 65 years of economic expansion. Yet, this revolution also underpinned the Cold War and more recently, distributed terror networks, cyberattacks, drone strikes, and the autonomous battlefields of the 21st century. Digital technology enabled unprecedented surveillance, precision targeting, and information warfare.
- **2020s - Biology is Next:** Biology has entered a similarly transformative era, much like the transistor moment in computing. Twenty years after the $2.7 billion Human Genome Project marked the beginning of the DNA reading era and scarcely ten years after DNA printing entered the marketplace at scale, CRISPR, low-cost DNA synthesis, and AI-guided protein design have turned cells into programmable hardware. This revolution offers immense potential: one-shot cures, drought-proof crops, carbon-eating bugs. However, the same toolkit scales risk and equips bad actors with new capabilities. Pathogen genomes can now be purchased, and viral misinformation spreads faster than the viruses themselves. The COVID-19 pandemic proved how biology can disrupt markets and erode trust; imagine the impact if this were deliberate or the result of a single mishandled sample in one of the growing number of Biosafety Level 3/4 labs now in

operation, or even irresponsible research in lower security labs—locations where research and development alone can cause massive danger.

The risk is existential. History teaches that every new discipline will be deployed in conflict; our job is to ensure that biological breakthroughs don't become our downfall. The anomaly in the human experience would be if we entirely prevented the use of biotech in human conflict or warfare. Biology is what we are and encapsulates everything around us on this planet. Without hyperbole, we believe that how humanity manages the biological engineering era is the most important new challenge of our time, only matched in scale with how we co-exist with artificial general intelligence. Our investment should be on the scale of nuclear deterrence.

Whether through malicious intent or reckless experimentation, evidence suggests that advanced biological capabilities will be tested in ways that threaten the safety of our societies. So, what do we do? The simple truth is that politics and norms alone have never stopped a new technological field from being used irresponsibly or weaponized. Very simply, we need to change our ambition to monitor and detect irresponsible or malicious activity. Our hypothesis is straightforward: We must focus massive attention on developing real-time, proactively generated biological intelligence—BIOINT. Like other domains, technical intelligence about the risk must become the core foundation of our response to this threat.

Just as satellite and ground-based monitoring established a powerful, layered system to monitor nuclear testing and capability development, comprehensive biosurveillance capabilities can enable attribution and dramatically shift the risk calculus for adversarial use of biological technologies. This foundational infrastructure creates a more stable global biosecurity

environment by providing the intelligence required to establish clear consequences for potential aggressors or irresponsible actors.

Strategic Requirement: *The West and its allies must deter and defeat any biological threat—natural or engineered. To do this, we must adopt a proactive strategy centered on rapid attribution and systemic resilience. Together, these create an enforcement architecture that dramatically reduces the risk of biological conflict.*

System Failure

The world has entered a new era of biological risk, yet our defenses remain outrun by rapid biotech innovation and out-maneuvered by adversaries. For half of a century, biodefense and biosecurity have depended on treaties and goodwill. They were the tools we had, but they are solutions that will not withstand the future. The WHO no longer commands authority in global health crises, and the Bioweapons Convention has proven unable to prevent multiple clandestine programs. Simply put, in an era of re-energized realpolitik, these institutions alone cannot provide the political power, surveillance, or real-time intelligence that modern biothreats demand.

How Adversaries Exploit our Failures:

- **Failure of the World Health Organization:** Created in 1948 to extend U.S. influence in a new world order, the World Health Organization (WHO) successfully helped the world respond to outbreaks and defeat infectious disease throughout the Cold War. Since then, it has succumbed to rivals who prize secrecy over transparency. Beijing now dominates key committees, withholds primary data, and delays on-site probes; Moscow amplifies disinformation that clouds every outbreak. The organization can still issue press releases

and framework agreements, but it cannot compel rapid sample-sharing or verify a lab incident in real time. In an era where hours count, the WHO provides no actionable BIOINT, no enforceable accountability, and thus no deterrence. Accordingly, Washington has lost the early-warning tool it once considered indispensable. The United States has therefore withdrawn, declaring its dissatisfaction with the return on American investment and highlighting the need for a new, nimbler framework—anchored to American interests—that can deliver real-time surveillance, accountability, and action.

- **Failure of the Biological Weapons Convention:** The 1972 Biological Weapons Convention (BWC) was supposed to lock in American-led norms against germ warfare, yet its negotiators left out intrusive inspections or continuous surveillance. Russia has violated it repeatedly, China hides vast dual-use work behind "civil-military fusion," and both governments veto every proposal to add verification clauses. By exploiting these loopholes—classifying research, denying foreign sampling, and stonewalling multilateral inquiries—they reduce the treaty to a paper shield even as they accelerate advanced biotech programs. Meanwhile, mid-tier states or even non-state actors can now engineer pathogens faster than the BWC's biennial meetings can be scheduled. Breakthrough tools such as CRISPR, AI-assisted protein design, and automated DNA printers only widen the gap between what proliferators can attempt and what the BWC can police. A political structure that cannot inspect, attribute, or punish simply hands proliferators plausible deniability while also robbing the West of the processes needed to deter or respond.

The Solution is Technical, Not Political

Political agreements, treaties, and conventions have a place, but we do not rely solely on those arrangements for nuclear security or cybersecurity. The biological domain is no different. We cannot continue to solely rely on diplomatic goodwill, a strategy that has already failed. Treaties still matter, but we need bold investments in data-driven platforms, real-time detection networks, and globally deployed operational capabilities to support their implementation. We need to work alongside allies to develop these capabilities in a trusted network.

The twin failures of the WHO and BWC illustrate the same immediate lesson: without a U.S.-anchored, technology-driven BIOINT system that can see, sample, and attribute in real time, political agreements alone will not thwart those who reject accountability.

BIOINT is Biosecurity

BIOINT is the capacity to place every microbial event on the map within hours. With this data comes attribution, with attribution comes deterrence: bad actors will not be able to move in silence – they will know we will prove who did it.

We Need Continuous Custody of Biological Data

At the dawn of the Cold War, visionaries like Dr. Edwin Land (then-CEO of Polaroid) championed aerial photography as a transformative tool for comprehensive intelligence. Today, biological data promises an even greater strategic impact—if we build the right infrastructure to harness it. We need continuous custody of global biological signals in a U.S.-anchored network that can identify potential outbreaks or engineered threats in near-real time. This means deploying a "Biothreat Radar" system worldwide: a persistent biosurveillance platform that

underpins our emerging BIOINT capabilities. We operationalize BIOINT through a global sensor layer, Biothreat Radar.

BIOINT is the Foundation of Biothreat Response

BIOINT is more than "better lab testing". It is a layered, continuous intelligence architecture that treats biology the way NORAD treats the sky: a globe-spanning network of Biothreat Radar sensors, clinical feeds, metagenomic sequencing, supply-chain telemetry, and open-source intelligence, all fused in a secure U.S.-anchored data hub. AI models continuously interrogate this stream for anomalies, forecast spread, and model countermeasures. The result is continuous custody of the world's microbial traffic—high-fidelity, time-stamped evidence that can be queried in minutes. Like satellite imagery for missiles, BIOINT provides "eyes-on" for every pathogen lineage, biosafety failure, research activity, and unexplained outbreak.

Fixing what the WHO and the BWC Cannot

Because BIOINT is technical, not diplomatic, it does the two things treaties now fail to do: verification and deterrence. With real-time sequence and metadata flowing to American allies globally, we no longer have to ask an adversary for samples or wait for politicized investigations; we can prove (or disprove) a lab origin within days and attribute malicious activity with forensic precision. Knowing they cannot hide, bad actors face immediate strategic costs—exactly the logic of deterrence that has kept nuclear weapons unused for 80 years. Equally important, BIOINT's shared dashboard gives allies a single, trusted picture of the microbial battlespace, replacing the information vacuum that paralyzed the WHO during COVID and that renders the BWC's paper prohibitions toothless.

Key Objectives for U.S.-led BIOINT include:

- **Near Real-Time Dataset Generation:** A U.S.-led, near real-time biointelligence data platform fusing pathogen genomics, environmental surveillance, and health data.
- **BIOINT as a Scalable Tech Challenge:** Treating biointelligence as a technology and data problem requiring significant scaling and AI-driven analysis.
- **Global Early Warning, Detection & Attribution:** Building a network that provides early warning of outbreaks, rapid identification of pathogens, and attribution capabilities.
- **Bilateral Surveillance Partnerships:** Launching engagements with key allied countries to serve as regional biointelligence nodes.

Comprehensive BIOINT doesn't just identify deliberate threats after release—it discourages their development and deployment in the first place. Attribution enables deterrence, and deterrence prevents catastrophe.

Biothreat Radar Blueprint

To complement current data sources and generate comprehensive BIOINT, we need newly deployed Biothreat Radar—a set of systems that create a single, version-controlled network that turns the planet into a living sensor grid.

Each node—whether an airport, border crossing, hospital, research lab, farm, or forward-deployed military unit—continuously samples wastewater, air, surfaces, and clinical feeds. Those raw signals flow through a common hardware-plus-software stack: automated prep benches, next-gen sequencers, and cloud pipelines that normalize metadata, time-stamp every read, and flag anomalies in real time. The moment any site uploads a new sequence or receives fresh threat intelligence, the platform pushes a "hot patch" across the entire constellation, updating primer sets, detection algorithms, and response playbooks in minutes.

Network Capabilities

The result is a self-synchronizing, responsive biosensing network, not a patchwork of laboratories, able to spot a novel microbe, trace its mutations, and ultimately alert decision-makers. Biothreat Radar integrates in real time:

- **Early warning:** Longitudinal baselines at critical nodes expose unusual genomic signatures before outbreaks explode into epidemics.
- **Unbreakable chain of custody:** Every sample, sequence, and analytic step is cryptographically logged, enabling fully transparent, auditable records.
- **Instant predictive capacity and countermeasure cueing:** Flagged sequences auto-populate threat models and feed in-house AI tools that design assays, diagnostics, and prototype vaccines within hours.

Interoperability and Allied Co-Ownership

Each Biothreat Radar node is designed to plug seamlessly into a federated architecture. Hardware standards, data schemas, and updated protocols are constantly versioned to every node in the network: Respect for national sovereignty gives partners full local authority over sampling, while shared APIs stream only the anonymized threat signatures required for collective early-warning. The result is a distributed "shield" rather than a U.S. only system, compatible with national control, able to snap into existing public-health infrastructure, and strengthened every time a new ally lights up a node. With Biothreat Radar in place, the United States and its allies shift from episodic outbreak response to persistent surveillance, gaining the reaction time—and evidentiary confidence—needed to deter, contain, and neutralize biological threats anywhere on Earth.

Beyond Detection: Building the Data Hub and Predictive Capabilities

Biothreat Radar must be more than a sensor grid; it must feed a secure, U.S-anchored data hub where every sequence, metadata tag, and environmental signal is standardized, time-stamped, and instantly shareable via API. This hub becomes the clearinghouse for global BIOINT, whether generated by Biothreat Radar or not, continuously merging field data with clinical records, trade flows, weather patterns, and livestock movements. Layered AI/ML models then convert those streams into predictive dashboards that can forecast case counts, spot anomalous mutations, and simulate how a pathogen would propagate through airline routes or supply chains. The same infrastructure is multipurpose and powers risk-scoring engines for insurers, daily "threat meters" for hospitals, and automated tasking of countermeasure R&D. In short, Biothreat Radar's always-on feeds generate the longitudinal baselines; the data hub fuses and cleans them; and predictive analytics turn them into actionable foresight, giving decision-makers the chance to block the next biological shock in a matter of days or weeks—not months.

Resetting Industry: America Needs a New Biosecurity Industrial Base

Achieving next generation biosecurity demands bold technological ambition; one that must be built and delivered by U.S. and allied industry. Newly developed Biothreat Radar and BIOINT systems need to be deployed and seamlessly integrated to support existing drug development and countermeasure research. True resilience comes from deterrence and rapid mitigation, proving the ineffectiveness of biological weapons. When a new computer virus strikes, threat detection and neutralization happens almost instantly on a global scale. Our biosecurity efforts should be just as agile. Whether a novel pathogen emerges in India or Indiana, decision-makers worldwide must receive actionable alerts within hours. That level of speed and

coordination demands trusted partners, real-time data flows, and integrated response tools. It's time the West and its allies built superior capabilities that respect individual freedoms and ensure we don't lose the next biological event.

The Biological Domain is the Last Frontier to Reboot

Anduril is rebooting defense for land, sea, and air. Palantir is leading an intelligence and industrial base reformation. SpaceX is transforming how we access and interact with the domain of space. The biological frontier needs its own category-defining pioneers. Such an ecosystem will unite Western data, hardware, and infrastructure to identify emerging biothreats and deploy rapid countermeasures in near-real time. We've been lucky so far—COVID excepted—but the relentless march of biotech means leaving it to chance will not suffice.

Government Partnership is Required to Keep Pace

We're at a pivotal moment. China sees biotech as a "strategic commanding height" in both economic and military realms and fuels state champions like BGI into massive expansion at Beijing's direction. Much like Huawei did with 5G, companies building a biotech industrial base for the Chinese state are forging ahead with massive global data collection programs and integrated R&D. Meanwhile, we and our allies have no similar structure to support the innovation and global integration required to safeguard freedom against biological threats.

We must build a biosecure nation and an allied ecosystem to match. We need a defense contracting ecosystem and a new breed of prime contractor that can seamlessly blend defense innovation and system integration.

What Capabilities Should We Require From a Biosecurity Industry?

In peacetime, the biosecurity industry builds a vital detection-and-data engine, collecting signals from around the world while being the "warm base" for outbreak response. The data generated enables protection of critical infrastructure and ultimately drives things like the development of tailored risk management products. The business opportunity expands beyond defense and offers coverage to critical infrastructure (airlines, ports, hospitals) and effectively quantifies the risk that no one else dares to underwrite while also mitigating the same. In wartime, the capability flips into rapid scale-up mode, deploying "rapid response chain" for defensive biology, mitigating an existential crisis before it cascades.

- **In Peacetime Mode: A Vital Detection & Data Engine**
    - Deploys Biothreat Radar stations worldwide to collect real-time pathogen data (wastewater, environmental samples, hospital feeds).
    - Generates BIOINT: a continuous, high-fidelity flow of genomic information that underpins modeling, early warning, and swift attribution.
    - Monitors signals from around the world and keeps capacity active, a "warm base" for outbreak response.
    - Generates the data that underpins critical-infrastructure protection (e.g., airports, subways, supply chains, hospitals).
    - Accurately quantifies risk for industries threatened by pandemics, engineered pathogens, or other biological threats.
- **In Wartime Mode: Rapid Scale & Crisis Containment**
    - Flips into high gear if a large-scale threat emerges, like a protective shield for biology.

- Activates a rapid response chain of defensive measures (sequencing, AI-driven triage, rapid prototypes of vaccines or therapeutics).
- Equips industry to develop defensive measures; distributes, deploys, and operates defensive infrastructure.

Owning the Pipeline from Threat to Countermeasure

A biosecurity industry manages the entire molecular data pipeline from detection to response. It performs high-throughput genomic sequencing of potential pathogens, uses AI to analyze this data for threat characterization, and rapidly develops proof-of-concept vaccines or treatments through computational and synthetic biology approaches. Once validated, these prototypes are licensed to U.S. and allied biotech partners for manufacturing. Throughout this process, companies across the industry maintain an integrated hardware-software stack through a global network—combining sampling stations, sequencing sites, cloud infrastructure, and analytics systems—all designed to meet a near real-time detection-to-response target for any emerging biological threat.

In sum, a next generation industry in biosecurity is building the technology required for the backbone of modern biosecurity: scanning the globe for suspicious signals and pivoting instantly from a quiet watch-stand to an all-out mobilization if danger strikes. Whether the next threat is a lingering microbe in an animal reservoir or a freshly engineered virus, the prime ensures no pathogen slips by unnoticed or without swift, robust response.

The Pipeline

- **Global Sensor Network**

    - Wastewater monitoring stations
    - Environmental air samplers
    - Clinical sample collection
    - Border/airport screening
    - Mobile field units
- **Secure Data Lake**
    - Real-time sequence uploads
    - Encrypted storage
    - Standardized metadata
    - Historical baselines
    - Cross-border feeds
- **AI Enabled Analytics Platform**
    - Anomaly detection algorithms
    - Mutation tracking
    - Spread prediction models
    - Risk scoring engines
    - Automated alerting
- **Rapid Attribution**
    - Source identification
    - Genomic forensics
    - Natural vs. engineered analysis
    - Chain of custody verification
    - Confidence assessment
- **Countermeasure Deployment**
    - mRNA vaccine templates
    - Diagnostic primer design
    - Therapeutic prototyping
    - Containment protocols
    - Strategic advisories

Economic Imperative

Biological threats are the most mispriced risk on earth:

- COVID-19 alone inflicted trillions of dollars of damage globally.
- Future pandemics or engineered pathogens could disrupt everything from supply chains to agriculture and manufacturing.
- The world allocates a mere fraction of defense and public health spending on infectious disease surveillance and testing.

Biology is not just a government concern—it's both a defense domain and a commercial commons. Industry needn't rely solely on government budgets. With accurate data and a scalable response system, a scaled biosecurity company could fix a massive problem of societal loss.

Estimated Economic Cost of the COVID-19 Crisis:

- **Lost GDP:** $7,592,000,000,000+
- **Premature Death:** $4,375,000,000,000+
- **Long Term Health Impairment:** $2,572,000,000,000+
- **Total Cost:** $16,121,000,000,000+
- **Total for a Family of Four:** $196,475

A Thriving Biotech Landscape, But a Missing "Horizontal" Industry Focus

Global biotech (therapeutics, diagnostics, industrial applications) already exceeds $1 trillion in market value, growing at double-digit rates. Airlines, ports, hospitals, and food producers all have immense vulnerability but no solutions. Western biotech remains fragmented, with each firm specializing in narrow drug pipelines or single platforms. We lack any integrated detection-and-response networks or robust risk-management products for pathogen-driven business threats.

The Fully Scaled Biosecurity Industry

A fully scaled biosecurity industry unites government and commercial markets by providing integrated detection and monitoring solutions, from airport bio-screening and military "subscriptions" (akin to missile defense) to year-round surveillance for hospitals, transit hubs, and food systems. On top of that, it offers national resilience packages (like a "100-Day Mission") for allied nations, bio-risk insurance for critical infrastructure, and real-time data for AIxBio—a unique global pathogen dataset that propels advanced therapeutics, agriculture, and public health. Down the road, it can fold in human augmentation programs, accelerating wound care or recovery therapies without compromising ethics, and enable reshored supply chains through novel bio-manufacturing, ensuring critical medicines and ingredients stay onshore.

The Path Forward

In the near term, we must begin by building core capabilities in BIOINT for America and allied governments—monitoring airports, military bases, and strategic sites with Biothreat Radar installations. As its network grows, our systems should naturally extend biosurveillance to commercial sectors like hospitals, agriculture, and manufacturing. From there, industry can leverage unique insights and data to launch bio-risk insurance programs, offering coverage for industries vulnerable to pandemics or engineered pathogens, and becoming a global bio-data broker for AI-driven drug discovery and public health analytics.

The Deployment Plan

We already see glimpses of this MVP: agencies such as the CDC, the Department of Defense (DoD), and governments in Qatar, the UK, Rwanda, Botswana, and Ukraine have partnered with the private sector to build new infrastructure enabling targeted detection. By

2028, we can scale such pilots into planet-wide networks capable of pinpointing and neutralizing emerging biological threats. By 2033, we must have 24-hour detection-and-response in much of the globe. Along the way, this infrastructure underpins bio-risk insurance and a robust data marketplace, fueled by comprehensive sequencing, risk modeling, and pathogen intelligence.

The Roadmap

Reaching this goal will require more than intent. It demands a clear, phased plan. In the coming months, we plan to define the step-by-step ambition needed to build toward 2033: what gets done when, by whom, and with what capabilities. This includes establishing concrete priorities and metrics to guide progress, such as the number of nodes monitored with Biothreat Radar, nations integrated into a BIOINT network, and self-reliance in countermeasure discovery and manufacturing.

By 2033, we must have 24-hour detection-and-response in much of the globe, drastically reducing the window for a pathogen to go from local outbreak to global crisis.

Ethical Safeguards

We do not believe there must be a trade-off between security, privacy, and prosperity. A century of experience, from air-traffic control to cyber-defense, shows that the surest path to freedom is pre-emptive protection: stopping disasters before they reshape society. Some safeguards are hyper-visible, like interceptors; others are almost invisible, like the firewalls that keep power-plants online. BIOINT should follow the same playbook, but with non-negotiable guardrails.

By baking these controls into the operating system from day one, we can build a biosurveillance shield that strengthens civil liberties instead of eroding them, turning the next generation of biosecurity tools into engines of both safety and democratic trust.

- **Privacy-by-Design architecture:** Biothreat Radar data will be encrypted in motion and at rest; processed with privacy-preserving analytics (federated queries, differential-privacy noise) so that actionable signals are generated without exposing personal information.
- **Layered, independent oversight:** A standing Public Biosecurity Board—drawn from civil-society groups, ethicists, and technical experts—should review sampling protocols, data-sharing agreements, and AI models before deployment. Independent audit logs ensure that accurate records of any dataset query are logged, enabling real-time redress if abuses are detected.
- **Dual-use safeguards and international norms:** All high-consequence work (e.g., multiplex assays that could reveal weaponizable genomes) is isolated in U.S. or allied facilities certified to the Federal Select Agent Program standard. At the diplomatic level, the United States commits to sharing non-sensitive BIOINT summaries with trusted allies, creating a verifiable deterrent without fueling an arms race.
- **Data sovereignty is paramount:** Biothreat Radar and the wider BIOINT infrastructure must be designed so that every participating nation can, by default, retain legal ownership and primary custody of the raw biological data collected within its borders - allowing such infrastructure to operate under established local privacy laws. Samples are processed in-country, stored in encrypted enclaves controlled by the host government, and only the minimal, pre-agreed metadata or anonymized analytic outputs are federated across the

network. This "sovereignty-first" architecture ensures that no state is asked to relinquish control of sensitive health information, while still allowing rapid, permissioned sharing of the specific signals needed for global early warning, attribution, and coordinated countermeasure development. In short, BIOINT protects borders as rigorously in the digital realm as any physical defense system, aligning with each nation's privacy laws and strategic interests while building the collective security shield we all require.

Building an Essential Capability for America and its Allies

COVID inflicted an almost unimaginable toll, dwarfing even major military expenditures. It will not be the last such event in our lifetimes. Thus, the next trillion-dollar frontier isn't solely in rockets or AI; it's biology, and control of this domain will shape the coming great-power era. We must not surrender that ground.

At Ginkgo Biosecurity, we've spent the past five years laying a foundation for next-generation biosecurity. We've demonstrated that large-scale biosurveillance powering BIOINT is possible, now we are on a mission to secure the biological frontier of the free world. We seek to secure our collective future against threats that could otherwise destabilize our societies.

No participant in this ecosystem is reinventing biotech's raw components; it's unifying them at scale. Together we're combining existing labs, AI pipelines, and global logistics into one biosecurity machine providing biosecurity for the planet. No single piece is novel; but the synergy and integration creates a unique asset.

Biology will decide the next great-power competition—and we must not cede the field.