Investigative Brief for FOIA Filing and Public Disclosure

Title: Palantir’s Synthetic Command Structure: A Technological Alignment with SOSA, MOSA, and Bio-Digital Surveillance Architecture

Author: April Preston / Alliance League Matching Services

Date: 5 June 2025

🧾 Executive Summary

This investigative brief presents compelling evidence that Palantir Technologies is operating in alignment with — and in many cases as the backbone of — a bio-cybernetic control grid architecture structured under the Department of Defense’s SOSA, MOSA, and Open Systems Architecture (OSA) mandates.

Despite public statements by Palantir CEO Alex Karp claiming the company does not “productize users” and upholds civil liberties, we find direct alignment between Palantir’s operational platforms (Gotham, Foundry) and a real-time surveillance and behavioral enforcement stack that now includes:

- Molecular communication systems (MC)
- Wireless Body Area Networks (WBAN)
- AI-driven behavioral scoring
- Blockchain-based access control
- Interoperable data fusion across federal agencies

This architecture violates both the spirit and letter of privacy rights, enabling pervasive biosurveillance and predictive enforcement against civilians under the pretext of health, safety, and efficiency.

Key Technologies in Use

Technology Layer	Function	Palantir’s Role
Molecular Communication (MC)	Signal delivery via mRNA, nanoparticles, optogenetics	Integration via NIH, HHS, DoD contracts
WBAN (Wireless Body Area Networks)	Body-worn & embedded sensor networks	Data ingest from wearable and implant telemetry
AI Behavioral Analysis	Interpretation of biosignals, emotion, intent	Foundry & Gotham applied to predictive risk modeling
Blockchain Identity Layer	Tokenized access to services based on behavior	Contracts in refugee ID, digital health tracking
SOSA / MOSA	DoD-mandated interoperability & modularity	

🔍 System Architecture Comparison

Field Map (2025): MC–WBAN–AI Interface Stack

vs.

*Palantir’s Operational Structure (2020–2025+)

Field Stack Component	Palantir Equivalency

Bio-nanomachine signal emitters	Body-worn biosensors (CDC, HHS, DoD)
Real-time WBAN broadcasting	IoMT / IoBT sensor integrations
AI scoring loops for behavior	Gotham predictive modeling (used by ICE, IRS, HHS)
Synthetic identity / biometrics	Digital Twin anchoring, biometric hash, facial recognition
Blockchain-based token gates	Verifiable Credentials (VC), DID integration pilots
Feedback-triggered stimulus	Algorithmic access control, medication dispensing via signal
Interoperability layer	SOSA-compliant sensor fusion platforms
Modular override/lockdown	MOSA-mandated modular enforcement contracts

Key Public Claims by Palantir CEO Alex Karp (Public Record)

Claim	**Fact-Check**

“We don’t productize users.”	False. Data is fused, scored, and used for automated access enforcement (IRS, ICE, HHS).
“Foundry is the most secure platform.”	Misleading. Granular access control exists on the front-end but behavioral AI sees full-spectrum fused data.
“Find anything erroneous in 90 seconds.”	Red Herring. The issue is not accuracy — it is systemic ethical misuse and predictive policing.

Confirmed Government Contracts

Agency	Project	Role
Department of Defense	JADC2, ABMS	Sensor fusion, behavioral modeling
HHS / CMS	Pandemic Response	Human biometric modeling, vaccine distribution
NIH / BARDA	Bio-countermeasures	Synthetic biology + AI modeling
IRS / Treasury	Taxpayer Data Fusion	Foundry integration for citizen-level analysis

ICE / DHS	Migrant tracking	Real-time behavior and location telemetry

Palantir’s Involvement with Behavioral & Physiological Surveillance

Examples of Use:

- ICE Enforcement & Removal: Real-time biosurveillance and migration path prediction
- CDC Pandemic Infrastructure: Vaccination risk prediction based on personal data streams
- IRS Foundry Deployment: Taxpayer behavioral risk profiling
- SSA Integration Talks: Behavioral and medical claims alignment
- Smart Contract Access: Blockchain-triggered access and denial (e.g. healthcare, employment, education)

Risk Summary

Concern	Impact
Privacy Violation	Merged biosensor, biometric, and behavioral data violates Fourth Amendment protections.
Surveillance Normalization	Permanent “health-justified” telemetry creates normalized biometric tracking.

Behavioral Enforcement	Predictive risk scoring tied to essential access = silent algorithmic governance.
Corporate-Government Overlap	Personnel overlap (DOGE + Palantir ties) creates undue private-sector influence on civil infrastructure.

FOIA Targets for Disclosure

Suggested FOIA requests:

1. All contracts, task orders, and SOWs (Statements of Work) between Palantir and:
   - Department of Homeland Security
   - Internal Revenue Service
   - Department of Health and Human Services
   - Department of Defense
   - Social Security Administration
   - Department of Education
2. Any internal communications between the Department of Government Efficiency (DOGE) and Palantir staff between 2019–2025 regarding:
   - Data interoperability efforts
   - Foundry or Gotham deployments
   - Biometric or physiological surveillance systems
   - Behavioral prediction algorithms
3. Security audits or reports regarding Foundry system access protocols and safeguards for biosignal data.

✊Concluding Statement for Public Publication

Palantir claims to be a protector of civil liberties. In truth, it provides the operational core for modular surveillance, bio-digital scoring, and real-time access enforcement using military-standard architectures originally designed for battlefield command.

Now, those systems are pointed at civilians — in the name of health, safety, and efficiency.

The evidence is clear:

This is not innovation. It is command and control.

It is not health. It is biometric domination.

It is not liberty. It is modular compliance through synthetic governance.

We must demand full transparency and halt this architecture before it becomes irreversible and normalized to tag, track, and tokenize (tax) humans without representation as though we are on a people farm.