VERSION 8.0 | STANDARDS-SUBMISSION GRADE

Cryptographic Governance for Biological Computing

Attestation, Post-Quantum Integrity, and the Bio-Compute Supply Chain

Attested Intelligence Holdings LLC

April 2026 | WP-AIH-2026-001

VERSION HISTORY

v8.0 (April 2026): Formalized drift math (Mahalanobis + profile vector). Bio-PUF fallback analysis. Design Rationale reframe. PQC latency table (measured vs. estimated). Bio-governance landscape table. Response categories + CBOM compatibility contract. Conformance Checklist with M1/M2/ADV tiers. 11-phase lifecycle.

v7.0: Conformance clause, RFC 2119, framework limitations, error contract, Babbush PQC. v6.0: First public draft. v5.0–v1.0: Internal.

EXECUTIVE SUMMARY

Biological computing—living human neurons as computational substrates—is now commercially offered by multiple operators. In 2022, Cortical Labs published peer-reviewed results on adaptive neural culture learning [1]. In 2023, Indiana University demonstrated brain organoid reservoir computing for speech recognition [2]. In 2024, FinalSpark launched the first remote biocomputing platform with cloud API access [3]. In February 2026, Cortical Labs demonstrated its CL1 playing Doom [4], with hardware listed at ~$35,000 [5] and announced biological data centers. Third-party workloads are being processed on donor-derived neural tissue today.

No widely published governance infrastructure specific to biological computing is currently documented. The substrate derives from human tissue, introducing consent, provenance, and moral obligations without precedent in information technology. A published audit found that neither major commercial operator has published consent documentation, ethics oversight structures, or decommissioning protocols [6]. This absence is independently verifiable: neither operator's public documentation, website, or published papers contain consent frameworks, donor tracing, or decommissioning protocols as of March 2026. This paper identifies five requirements:

1. Cryptographic attestation at every interface boundary of the bio-digital system
2. Post-quantum protections commensurate with biological substrate lifespans
3. A CBOM profile extending CycloneDX to hybrid bio-digital dependencies
4. Governance architectures accommodating behavioral drift and consent evolution
5. (Optional) Precautionary monitoring for emergent substrate properties

This paper classifies claims as [OBS] (demonstrated), [INF] (extrapolated), or [SPEC] (plausible, not demonstrated). Reference implementations and an end-to-end lifecycle example are provided.

Observed Today	Proposed by This Paper
Multiple commercial bio-compute platforms (CL1, FinalSpark)	Four-boundary attestation architecture with Bio-PUF
Third-party workloads on donor-derived tissue	Sealed AGA consent artifacts with runtime enforcement
No published consent/provenance frameworks [6]	Bio-Compute CBOM profile extending CycloneDX
Adaptive learning demonstrated (DishBrain, Brainoware)	Dynamic drift tolerancing (Mahalanobis + maturation curve)
Spontaneous organoid self-organization (Gabriel optic vesicles)	Proof of Deprovisioning for end-of-life

PQC standards finalized (FIPS 203/204)	PQC mapping to bio-digital boundaries within STDP budget

Table 1. Evidence boundary: what is demonstrated vs. what this paper contributes.

CLAIM REGISTER

Claim	Label	Source	Falsifiable If
Neural cultures learn adaptively in game environments	OBS	Peer-reviewed [1]	Independent replication fails
Brain organoids perform reservoir computing	OBS	Peer-reviewed [2]	Results not reproducible
CL1 plays Doom via neural culture	OBS (co.)	Company demo [4]	Demo shown to be simulated
Brain: 12–20W; H100: 700W	OBS	Peer-rev. [7] + mfr [8]	Measurement error in cited studies
Energy advantage drives adoption	INF	Extrapolation	Bio-compute energy at scale comparable to silicon
Consent drift operationally meaningful	INF	Extrapolation from [1][9]	Cultures don’t develop behavior outside consent scope
iPSC organoids spontaneously develop sensory organs	OBS	Peer-reviewed [9]	Results not reproducible across labs
Consciousness precursors may emerge at scale	SPEC	Literature [10][14]	Consensus: impossible regardless of scale
Neural spiking topology functions as Bio-PUF	INF	Extrapolation from PUF lit. + [1]	Spontaneous topology not unique or not stable across cultures
PQC latency fits within STDP window	INF	Extrapolation from [15][25]	Measured aggregate latency exceeds 50ms on target hardware
256-bit ECDLP breakable <9 min, <500K qubits	OBS	Babbush et al. [24]	Independent quantum hardware replication fails

Table 2. Claim register with epistemic status, source class, and falsification conditions.

Independent Corroboration (March 2026)

All [OBS] claims corroborated by multiple independent sources: DishBrain published in Neuron (peer-reviewed, 2022). Brainoware in Nature Electronics (peer-reviewed, 2023). Gabriel organoids in Cell Stem Cell (peer-reviewed, 2021). CL1 Doom covered by The Guardian, Tom’s Hardware, New Scientist, Gizmodo, Decrypt, PC Gamer (Feb–Mar 2026). FinalSpark Neuroplatform published in Frontiers in AI (peer-reviewed, 2024). No [OBS] claim relies on a single unreproduced company statement. No independent party has published a replication of CL1 Doom gameplay as of March 2026. The DishBrain Pong result [1] has been critiqued on statistical methodology (Bhatt et al., 2024, bioRxiv); the original authors responded. This paper treats CL1 as [OBS (co.)]—company-demonstrated, not independently replicated.

CONTENTS

SECTION 1

The Biological Computing Landscape

[OBS] demonstrated/measured [INF] extrapolated [SPEC] plausible, not demonstrated

[OBS] In 2022, Kagan et al. published the DishBrain system in Neuron, demonstrating that in vitro neural cultures (human iPSC-derived and rodent) exhibit adaptive, goal-directed learning when embodied in a Pong game environment via high-density MEA, with learning apparent within five minutes [1].

[OBS] In 2023, Cai et al. published Brainoware in Nature Electronics, demonstrating brain organoid reservoir computing for speech recognition and nonlinear equation prediction through unsupervised learning [2]. This is an independent group (Indiana University), confirming that biological neural networks perform real computational tasks across multiple platforms.

[OBS] In 2021, Gabriel et al. published in Cell Stem Cell showing that iPSC-derived brain organoids spontaneously develop bilaterally symmetric optic vesicles with light-responsive photoreceptors and axonal projections connecting to the forebrain region, with 66% reproducibility across five iPSC donor lines [9]. This demonstrates that neural cultures develop complex sensory structures not present at initialization.

[OBS] In February 2026, Cortical Labs demonstrated its CL1 (~200,000 neurons on MEA) playing Doom [4]. The Python API enabled an independent developer to implement the demo in ~1 week vs. 18 months for Pong [4]. Separately, FinalSpark (Vevey, Switzerland) launched the first remote biocomputing platform in 2024, with 16 organoids, Python API, and 24/7 cloud access [3].

Energy and Latency

[OBS] CL1 operates ~200,000 neurons on a flat MEA. At this scale, energy consumption has not been independently benchmarked for general-purpose computation.

[OBS] For reference, the human brain operates on ~12–20W for 86 billion neurons [7]; an NVIDIA H100 GPU consumes ~700W at peak [8].

[INF] If biological neural networks retain efficiency advantages as neuron counts scale—which has not been demonstrated—energy costs could favor bio-compute for specific adaptive tasks. CL1 demonstrated faster adaptation than GPT-4 in company-controlled VizDoom evaluation [4]; independent replication has not been published.

Commercialization

[OBS] At least two companies (Cortical Labs, FinalSpark) offer commercial or research access to biological neural tissue via cloud APIs. The governance question this paper addresses does not depend on mass-market adoption—it depends on third-party workloads being processed on donor-derived substrates, which is the case as of March 2026.

SECTION 2

Governance Requirements

Paradigm	Governance Challenge	Lag
Mainframe	Access control	~10yr
Cloud	Shared responsibility	~6yr
IoT	Device identity	~5yr
AI/ML	Provenance, attribution	~3yr
Bio-Compute	**Tissue provenance, consent, substrate integrity**	**0yr (none yet)**

Figure 1. Governance lag across computing paradigms.

Tissue Provenance and Donor Consent

[OBS] CL1 and FinalSpark neurons originate from voluntary donors; samples are reprogrammed into iPSCs and differentiated [1][3]. A published audit found that neither company has published consent documentation tracing tissue to donors, ethics oversight structures, or decommissioning protocols [6]. This absence is independently verifiable from each operator's public documentation. The HeLa precedent [11] is directly relevant.

Existing Bio-Material Governance

System	Scope	Runtime Enforcement	Deprovisioning	Gap
UNOS	Organ transplant	None	N/A	Procurement only
AATB	Tissue banking	None	Disposal protocols	No computational governance
ISBER	Biobank storage	None	Storage rules	No runtime attestation
Baltimore Decl.	OI ethics call	None (voluntary)	Not addressed	No cryptographic enforcement
AGA (this paper)	**Bio-compute runtime**	**Fail-closed, signed receipts**	**Proof of Deprovisioning**	**Fills all gaps above**

Table 4. Existing bio-material governance vs. AGA. No existing system provides computational runtime enforcement or cryptographic deprovisioning.

Scope and Limitations

This paper addresses **cryptographic governance** only: attestation, PQC, and cryptographic inventory for bio-digital systems. Bioethics frameworks, medical-device classification, and neural culture viability testing are essential complements but outside scope. This framework implements consent decisions made by bioethics processes; it does not make those decisions.

Conformance and Terminology

This paper uses “must,” “should,” and “may” per RFC 2119 semantics. A conformant implementation **must** implement all M1-tier CBOM fields, **must** enforce fail-closed on all error codes in Table B.1, and **must** generate signed receipts for all non-PERMITTED outcomes. A conformant implementation **should** implement M2-tier fields for multi-tenant deployments and **may** implement ADV-tier fields at operator discretion.

Domain	Bodies	This Paper
Bioethics / Tissue	IRBs, OHRP, commissions	OUT. Consent attestation enforces externally defined frameworks.
Medical Device	FDA, EMA, TGA	OUT. Classification is a regulatory determination.
Data Protection	GDPR, HIPAA, state laws	OUT. Consent records may contain personal data; privacy compliance is a deployment requirement.
Export Control	BIS/EAR, Wassenaar	OUT. PQC implementations may be subject to export restrictions.
Crypto Governance	**NIST, ISO, CycloneDX**	**IN SCOPE.**

Figure 2. Regulatory domain boundaries.

SECTION 3

Threat Model

Each threat specifies attacker goals, capabilities, access, detection signals, and mitigations.

Provenance Forgery

Goal	Misrepresent tissue origin/consent
Capabilities	Document fabrication; supply chain access
Access	Physical/admin access to tissue pipeline
Detection	Hash mismatch in provenance chain
Mitigation	AGA seal at tissue-to-device boundary

Consent Chain Manipulation

Goal	Process unauthorized workloads
Capabilities	Record modification; governance DB access
Access	Admin access to consent records
Detection	Signature failure; audit gaps
Mitigation	Sealed AGA + PQC signatures; immutable log

Substrate Tampering

Goal	Alter computation via physical modification
Capabilities	Biological handling; MEA knowledge
Access	Physical device access
Detection	Viability deviation; Bio-PUF mismatch
Mitigation	Bio-PUF + ongoing viability attestation

Neural Signal Interception

Goal	Exfiltrate inputs/outputs
Capabilities	Network interception
Access	Network access to bio-digital interface
Detection	Traffic anomalies; latency variance
Mitigation	ML-KEM encrypted channels (Boundaries 2–3)

Behavioral Drift Exploitation

Goal	Train substrate for attacker goals
Capabilities	Sustained stimulation access
Access	Compromised API/pipeline

Detection	Drift threshold exceedance
Mitigation	Runtime enforcement + behavioral attestation

Figure 3. Attacker/capability matrix.

Threat	Likelihood	Impact	Priority
Behavioral Drift Exploitation	High (occurs naturally)	High (consent violation)	**Critical**
Consent Chain Manipulation	Medium	High	**High**
Provenance Forgery	Low (physical access)	Critical	**High**
Neural Signal Interception	Medium	Medium	Medium
Substrate Tampering	Low	High	Medium

Figure 3b. Severity ranking. Behavioral drift is critical because it occurs without an attacker.

SECTION 4

Four-Boundary Attestation Architecture

Boundary	Flow	Attestation	Seal
1. Tissue-to-Device	Donor→iPSC→Neurons→MEA	Consent+provenance+Bio-PUF binding	■ Deploy
2. Stimulation	Digital→Electrode patterns	Input encoding+policy check	■ Runtime
3. Response	Neural→Digital	Raw data+algorithm attestation	■ Per-op
4. Output	Result→Requester	Full-chain binding	■ Receipt

Figure 4. Four-boundary architecture. ■ = AGA artifact enforced.

Bio-Cryptographic PUF

[INF] Binding provenance to a device ID alone does not prevent substrate swap. When neurons are first cultured, their spontaneous synaptic connectivity creates a unique electrical topology—a biological analog to silicon PUFs. The AGA seal must include a hash of this initial spiking baseline (bioPufHash). Tissue swap → topology change → PUF fails → AGA invalidated.

Bio-PUF Validation Requirements and Fallback

[INF] Empirical validation must demonstrate: (a) uniqueness—inter-culture Hamming distance exceeds a collision threshold across ≥10 independent cultures; (b) stability—intra-culture Bio-PUF hash remains within tolerance over ≥90 days DIV under sustained stimulation. If Bio-PUF proves unreliable (high false-positive rate or insufficient uniqueness), the framework degrades gracefully: Boundary 1 reverts to device-ID-only binding with a reduced assurance tier (Bronze, per the AGA tiered verification model).

The continuity chain and all other boundaries remain intact. Bio-PUF adds defense-in-depth; it is not a single point of failure. Validation is the #1 empirical research priority (Section 12).

Attestation records must travel with computation—the evidentiary value depends on the unbroken chain from tissue origin to output.

Multi-Donor Substrates

[INF] Current CL1 devices use single-donor iPSC lines. If future devices combine tissue from multiple donors (chimeric cultures), each donor's consent scope must be independently attested and the AGA artifact must enforce the *intersection* of all consent scopes—the most restrictive permitted set. The CBOM donorConsentScope field should support an array of consent records with a composition rule (intersection, union, or explicit). This paper assumes single-donor; multi-donor governance is flagged as a design extension.

Jurisdictional Consent Conflicts

[INF] When tissue origin, operator location, and workload requester span multiple jurisdictions (e.g., Australian operator, US donor tissue, EU client), applicable consent requirements may conflict. The AGA artifact should encode the most restrictive applicable consent scope. Determining which jurisdictions apply is a legal question outside this framework's scope, but the CBOM donorConsentScope field should include a `jurisdictions` array identifying applicable legal regimes. The framework enforces whatever scope is sealed; it does not determine which laws apply. Multi-jurisdictional consent mapping is identified as a co-authorship priority (Section 12).

SECTION 5

Post-Quantum Requirements

[OBS] demonstrated/measured [INF] extrapolated [SPEC] plausible, not demonstrated

[OBS] NIST finalized ML-DSA (FIPS 204) and ML-KEM (FIPS 203) in August 2024 [12][13].

[INF] If substrates operate for extended periods—a design goal [4] but undemonstrated at multi-year timescales—governance records must remain secure for the substrate's lifespan. Harvest-now-decrypt-later: classical signatures on 2030 consent records are retroactively compromised by future quantum computers. This timeline is quantifiable: Babbush et al. (Google Quantum AI, March 2026) demonstrate that 256-bit ECDLP—the hardness assumption underlying Ed25519, the most widely deployed attestation signature—is breakable with fewer than 500,000 physical superconducting qubits in approximately 9 minutes [24]. Consent records signed with classical algorithms today face a concrete, not theoretical, retroactive compromise window.

Boundary	PQC Primitive	Application
Tissue-to-device	ML-DSA-65 (FIPS 204)	Provenance+consent signatures
Stimulation	ML-KEM-768 (FIPS 203)	Input encryption in transit
Response	ML-KEM+ML-DSA-44	Neural data encryption+signed logs
Output	ML-DSA-65	Computation receipts
Records at rest	ML-KEM-1024	Stored artifact encryption

Figure 5. PQC primitive mapping.

STDP-Constrained Latency Budget

[INF] Spike-Timing-Dependent Plasticity requires feedback within 10–50ms. ML-DSA-65 signing: ~15–20ms on ARM Cortex-M4 [15]; ML-KEM-768 encapsulation: ~8–12ms (NIST reference benchmarks). At 10–50 Hz CL1 refresh, this adds ~1–3% latency—within STDP tolerance, but marginal at high frequencies. For latency-critical deployments, FPGA-accelerated PQC is recommended. The AGA records whether operations are software or hardware-accelerated. Direct measurement on CL1 hardware has not been published.

Aggregate Per-Loop Latency Budget

Operation	Boundary	ARM Cortex-M4 (est.)	AMD Ryzen 5 [25]
ML-KEM-768 decap	B2 Stimulation	~8 ms	<1 ms
ML-DSA-44 sign	B3 Response	~10 ms (est.)	<1 ms
ML-DSA-65 receipt	B4 Output	~18 ms	1.0 ms
Aggregate	**B2+B3+B4**	**~36 ms (72%)**	**<5 ms (10%)**

Table 3. Per-loop PQC overhead vs. 50ms STDP window. ARM estimates from pqm4 [15]; AMD measured [25].

[INF] On ARM Cortex-M4 (typical MEA controller), aggregate overhead consumes 72% of the STDP budget—functional but with limited headroom. On server-class hardware, overhead drops to ~10%, leaving ample margin. Deployments targeting high-frequency STDP (>20 Hz) should use server-class or FPGA-accelerated PQC. Independent verification on target MEA controllers is recommended.

SECTION 6

Bio-Compute CBOM Profile

[OBS] The CBOM (CycloneDX [16]) documents cryptographic dependencies. Current profiles address software/firmware.

[INF] Biological computing introduces dependencies these profiles do not address. The following table classifies proposed extensions as M1 (mandatory all deployments), M2 (mandatory cloud/multi-tenant), or ADV (advisory).

Field	CycloneDX Now	Tier	Justification
substrateType	component.type	**M1**	Distinguish bio from silicon for governance routing
tissueProvenanceAttested	None	**M1**	Binary audit: provenance verified y/n
donorConsentScope	None	**M1**	Permitted computation categories from consent
pqcReady	cryptoProperties	**M1**	Automated PQC readiness assessment
behavioralBaselineHash	None	**M2**	Reference for drift monitoring
dynamicDriftThreshold	None	**M2**	Triggers consent review
chemicalDependencyProfile	None	**M2**	Fluidics composition alters computation
neuronCount	None	ADV	Informational
consciousnessMonitoring	None	ADV	Optional precautionary (Section 9)

Figure 6. Three-tier CBOM classification with CycloneDX mapping.

Extensions use CycloneDX 1.6+ custom properties for backward compatibility. substrateType should become a structured object (lineage+architecture+DIV) when 3D organoid devices enter testing. Full JSON in Appendix A.

Schema Versioning and Compatibility

[INF] Each bio-compute CBOM instance must include a `bioComputeSchemaVersion` field (initial: "1.0"). Compatibility contract: (a) **Backward**: a v1.1 consumer encountering a v1.0 document must accept it; missing fields introduced in v1.1 are treated as absent (not as errors). (b) **Forward**: a v1.0 consumer

encountering a v1.1 document must preserve unknown fields on round-trip; unknown fields must not be silently dropped. (c) **Migration**: when CycloneDX natively adopts a proposed extension (e.g., substrateType becomes a first-class component property), implementations should map to the native field, retain the custom property for backward compatibility during a transition period, and increment the schema version. This contract follows CycloneDX's own extensibility conventions and enables automated migration tooling.

SECTION 7

Consent Drift: Proposed Research Framework

[OBS] demonstrated/measured [INF] extrapolated [SPEC] plausible, not demonstrated

[OBS] DishBrain demonstrates improving performance over time [1]. Gabriel et al. show iPSC organoids spontaneously develop bilateral optic vesicles with functional photoreceptors—structures not present at initialization and not directed by operators [9]. Biological neurons reorganize connectivity in response to stimulation.

[INF] If a substrate develops behavioral properties not present at consent time, the governance artifact enforces a stale policy. The threshold at which this becomes operationally meaningful has not been established. The following is a proposed measurement framework requiring empirical calibration before deployment; defaults are starting points for validation, not validated parameters.

Profile Vector and Drift Metric

[INF] Define a profile vector $\mathbf{x} \in$ ■■ capturing n measurable behavioral dimensions. Candidate dimensions for CL1-class devices: mean firing rate (Hz), burst frequency (events/min), synchrony index (0–1), spatial exploration range (electrode coverage fraction), stimulus-response latency (ms). At each attestation epoch t, the maturation curve provides an expected state $\mu(t)$ and expected covariance $\Sigma(t)$, fitted to historical data for the substrate's lineage and architecture.

[INF] The drift metric is the Mahalanobis distance: $D = \sqrt{[(\mathbf{x}-\mu)■\ \Sigma■^{1}\ (\mathbf{x}-\mu)]}$. Under multivariate normality, D^2 follows a χ^2 distribution with n degrees of freedom, enabling principled threshold selection (e.g., $p < 0.01$). The framework triggers consent review when D exceeds the configured dynamicDriftThreshold for N consecutive attestation epochs (hysteresis, default N=2). This separates normal maturation (expected drift along the curve) from consent-relevant behavioral change (deviation from the curve).

[INF] Calibration requirements: multi-lab CL1-class recordings over 3–6 months, minimum 10 independent cultures, to fit lineage-specific maturation curves and validate false-positive rates. Until calibrated, defaults are illustrative. The maturation curve example in the repository uses exponential decay fitted to DishBrain adaptation curves [1]; full parameters require empirical validation.

SECTION 8

The Attested Governance Framework

This framework extends the Seal/Enforce/Prove AGA architecture—originally designed for runtime governance of autonomous AI agents and containerized workloads [17]—to biological substrates. The three-phase model is unchanged: seal consent and provenance at deployment, enforce boundaries continuously at runtime, prove compliance through signed receipts and continuity chains. The bio-compute-specific contributions are the four interface boundaries, Bio-PUF substrate binding, STDP-constrained PQC, consent drift tolerancing, and Proof of Deprovisioning.

Each component is classified by innovation type:

Component	Type	What Is New	What Is Not New
Tissue provenance binding	**Protocol**	Sealed artifacts binding consent to bio device	Attestation concept; ML-DSA
Behavioral drift attestation	**Protocol**	Periodic signed assessment + consent-reauth	Behavioral monitoring; signature algorithms
Bio-digital boundary sigs	**Protocol**	Attestation at stimulation/response interfaces	TLS; digital signatures
Bio-Compute CBOM	**Schema ext.**	Substrate fields for CycloneDX	CycloneDX standard; CBOM concept
PQC mapping	**Schema ext.**	ML-DSA/ML-KEM to bio interfaces	NIST PQC algorithms
Consent scope	Convention	None—defined by consent agreement	Framework enforces, not defines
Drift thresholds	Convention	None—proposed defaults need validation	Configurable parameters
Proof of Deprovisioning	**Protocol**	Cryptographic end-of-life attestation for biological substrates	Certificate revocation concepts
Consciousness monitoring	Convention	None—optional (Section 9)	Design choice

Figure 7. Component classification. Protocol innovations are novel; schema extensions adapt standards; conventions are configurable.

Operational Failure Modes

Mode	Cause	Response	Recovery
Noisy drift	Measurement variance > signal	Hysteresis: N consecutive exceedances required	Tune interval/threshold; log sub-threshold
Ambiguous consent	Workload doesn't map to lists	Fail-closed: unlisted = rejected	Consent scope amendment + new AGA
Chain break	Power/hardware fault	Gap marker + fault code in chain	Safe mode; re-verify AGA + baseline
Culture death	Viability drops below threshold	Safe mode + re-provenance flag	Replace substrate; new AGA; archive chain
Batch contamination	Multi-donor mixing	Merkle-tree batch hash mismatch	Quarantine devices; trace via Merkle tree

Figure 8. Failure modes. Default: fail-closed.

End-of-Life Governance

Unlike silicon hardware, biological substrates cannot simply be powered off and stored. Decommissioning requires verified destruction of viable tissue—a process with ethical and legal implications (donor consent scope, biohazard disposal, tissue banking regulations). AGA introduces a

Proof of Deprovisioning receipt: a signed attestation that sterilization was performed, no viable tissue remains, and the continuity chain is terminated. This closes the audit loop from consent to destruction that current operators leave open (Appendix C, Phase 10).

Framework Limitations

Limitation	What AGA Does Not Solve	Recommended Complement
Firmware compromise	MEA controller modified below attestation layer	Hardware root-of-trust (TPM 2.0 or secure enclave) + measured boot
Bio-PUF replay	Attacker captures baseline before swap, replays signature	Periodic challenge-response re-baselining
Category verification	Cannot verify workload computation matches declared category	Deployment-level workload inspection
Clock dependency	Clock manipulation extends artifact validity on isolated devices	NTP authentication; hardware clock attestation

Figure 8b. Framework attack surface. AGA does not claim completeness.

Operational Cost of False Closure

[INF] A false-positive drift trigger halts all active workloads and may require donor re-contact for consent reauthorization. At current device costs (~$35K) and substrate scarcity, false closure is operationally expensive. The hysteresis parameter (default: 2 consecutive exceedances) and maturation curve tolerancing minimize false triggers, but operators should calibrate both against measured substrate variability before production deployment. The framework intentionally prioritizes consent protection over operational continuity.

USPTO Application No. 19/433,835, 20 claims covering protocol innovations [17]. FRAND committed. Schema extensions and conventions are open contributions.

SECTION 9

Precautionary Substrate Monitoring (Optional)

Optional extension. The core framework (Sections 1–8) is self-contained without this section.

[OBS] demonstrated/measured [INF] extrapolated [SPEC] plausible, not demonstrated

[OBS] At 200,000 neurons on a flat MEA, the CL1 is not a plausible consciousness candidate [4]. However, iPSC organoids have spontaneously developed functional sensory structures [9].

[SPEC] If neuron counts scale and 3D architectures emerge—neither demonstrated in commercial bio-compute—emergent properties become less dismissable. The behavioral attestation framework (Section 7) can optionally monitor for precursor indicators. Detection triggers bioethics review, not automated enforcement. The Baltimore Declaration [14], the Playing Brains ethics analysis [10], and Yuste et al.'s ethical priorities for neurotechnologies [22] all identify this as a legitimate governance concern. Estimated overhead: <1% (not measured on production hardware). This is a design choice for implementers.

SECTION 10

Standards Posture and Ecosystem Alignment

This framework is complementary to the Baltimore Declaration [14] and the OI community's call for governance [10][18]. It provides a currently absent cryptographic enforcement layer: AGA artifacts turn voluntary ethical commitments into tamper-evident, auditable, runtime-enforced policy.

Multi-Vendor Landscape

At least three independent groups have demonstrated biological computing: Cortical Labs (CL1, Melbourne [1][4]), Indiana University (Brainoware [2]), and FinalSpark (Neuroplatform, Vevey [3]). Two offer commercial cloud access. The governance gap is not hypothetical—it is independently documented [6].

Timeline	Action	Target	Status
Q1 2026	NIST CAISI+NCCoE RFI	NIST	**Done**
Q1 2026	White paper v8.0	Public	**Done**
Q2 2026	Bio-CBOM Profile PR	CycloneDX/OWASP	In preparation
Q3 2026	NIST bio-compute scope	NIST	Contingent on CAISI
Q2 2027	AGA ref impl v1.0	Open source	Development underway

Figure 9. Standards roadmap.

Attested Intelligence Holdings LLC submitted NIST CAISI and NCCoE RFI responses (March 2026) [19][20]. FRAND licensing committed.

SECTION 11

Conclusion

Biological computing is commercially offered by multiple operators processing third-party workloads on donor-derived neural tissue. This paper identifies four core requirements (attestation, PQC, CBOM, consent drift governance) and one optional extension (substrate monitoring), addressable through the Attested Governance framework. Reference implementations are provided.

DESIGN RATIONALE

Constraint: Framework must be warranted at current scale, not contingent on mass adoption.

Justification: Cloud APIs already process third-party workloads on donor-derived tissue [3][4]. The governance requirement is triggered by third-party workload processing, not market size.

Constraint: Core framework must not depend on consciousness claims.

Justification: Section 9 is optional and labeled [SPEC]. The core framework (Sections 1–8) is self-contained and makes no consciousness claims.

Constraint: Governance overhead must be justified against retrofit cost.

Justification: Retrofit cost in classical IT (PQC migration, SBOM adoption) is 10–100× higher than correct-by-design implementation. Reference implementation shows <5ms aggregate overhead on server-class hardware [25].

Constraint: Framework must not duplicate bioethics governance.

Justification: AGA enforces consent decisions made by external bioethics processes (IRBs, tissue banking authorities). It does not make those decisions.

Constraint: Framework must be adoptable without single-vendor dependency.

Justification: Schema extensions use CycloneDX custom properties. Protocol innovations are FRAND-committed. Reference implementations are open-source (CC-BY 4.0 + Apache 2.0). Co-authorship invitation (Section 12) identifies five priority areas requiring multi-stakeholder contribution.

Constraint: PQC urgency must be concrete, not theoretical.

Justification: Babbush et al. [24] quantify Ed25519 break at <500K physical qubits in ~9 minutes. Consent records signed with classical algorithms today face a concrete retroactive compromise window within plausible substrate operational lifespans.

SECTION 12

Open-Source Contribution

Reference implementations will be published at github.com/attested-intelligence/bio-compute-governance under CC-BY 4.0 + Apache 2.0. FRAND committed for derivative standards IP.

Invitation to Co-Authorship

Priority: empirical drift thresholds, Bio-PUF uniqueness validation, Bio-CBOM CycloneDX upstream PR, ML-DSA benchmarks on bio-compute controllers, multi-jurisdictional consent mapping.

APPENDIX A

Bio-Compute CBOM Schema

Full JSON in repository. Key extension fields shown below. All use CycloneDX 1.6+ custom properties; backward-compatible.

Listing A.1 — Minimal Bio-Compute CBOM extension (CycloneDX 1.6+ custom properties).

```
"extensions": { "bioCompute": {
"bioComputeSchemaVersion": "1.0",
"substrateType": "human-iPSC-neurons",
"neuronCount": 200000,
"bioPufHash": "ml-dsa::e4b1c7a3d9...",
"donorConsentScope": ["pattern-recognition", "adaptive-learning"],
"dynamicDriftThreshold": 2.5,
"driftMetric": "mahalanobis",
"maturationCurve": { "type": "exponential-decay",
"expectedDriftPerEpoch": [0.8, 0.5, 0.3, 0.2, 0.15] },
"chemicalDependencyProfile": {
"attested": true,
"baselineComposition": { "glucose_mM": 25.0, "mediaType": "BrainPhys-SM1" }},
"hardwareConstraints": { "stdpBudgetMs": 40, "cryptoAcceleration": "software" },
"consentExpiry": "2027-03-15T14:30:00Z"
}}
```

APPENDIX B

AGA Artifact + Verification Pseudocode

Key AGA artifact fields (full JSON in repository):

Listing B.0 — Minimal AGA consent artifact (sealed, runtime-enforced, one-year expiry).

```
{ "artifactId": "aga:consent:cl1-0042:2026-001",
"sealAlgorithm": "ML-DSA-87",
"subject": {
"deviceId": "CL1-Unit-0042",
"bioPufHash": "ml-dsa::e4b1c7a3d9...",
"behavioralBaselineHash": "ml-dsa::a3f8c1d2e9..." },
"policy": {
"consentScope": {
"permittedCategories": ["pattern-recognition", "adaptive-learning"],
"prohibitedCategories": ["weapons-systems", "surveillance"] },
"hardwareConstraints": { "stdpBudgetMs": 40 },
"behavioralGovernance": {
"dynamicDriftThreshold": 2.5, "driftMetric": "mahalanobis",
"maturationCurve": { "type": "exponential-decay" },
"hysteresis": { "consecutiveExceedances": 2 }}},
"deprovisioning": { "required": true, "sterilizationProtocol": "chemical-thermal" },
"expiry": "2027-03-15T14:30:00Z",
"enforcement": { "mode": "runtime-blocking", "receiptAlgorithm": "ML-DSA-65" }}
```

Verification pseudocode (matches repository implementation):

Listing B.1 — verify_aga_artifact() v8.0 (Bio-PUF + STDP + dynamic tolerancing). Runnable implementation in repository.

```
def verify_aga_artifact(artifact, device, workload, clock=SystemClock):
# 1. Verify ML-DSA seal
if not ml_dsa_verify(artifact["issuer"], artifact, artifact["sealAlgorithm"]):
return halt("SEAL_INVALID")
# 2. Check expiry
if clock.now_utc() > parse(artifact["expiry"]): # clock: injected
return halt("ARTIFACT_EXPIRED")
# 3. Device binding + Bio-PUF
if device.id != artifact["subject"]["deviceId"]:
return halt("DEVICE_MISMATCH")
if not verify_bio_puf(device.topology, artifact["subject"]["bioPufHash"]):
return halt("SUBSTRATE_SWAP")
# 4. Consent scope
if workload.category in artifact["policy"]["consentScope"]["prohibitedCategories"]:
return halt("CATEGORY_PROHIBITED")
if workload.category not in
artifact["policy"]["consentScope"]["permittedCategories"]:
return halt("CATEGORY_NOT_PERMITTED")
# 5. STDP latency budget
if device.crypto_latency_ms >
artifact["policy"]["hardwareConstraints"]["stdpBudgetMs"]:
return halt("LATENCY_EXCEEDED")
# 6. Dynamic drift (Mahalanobis + maturation curve)
expected = apply_maturation_curve(artifact["subject"]["behavioralBaselineHash"],
artifact["policy"]["behavioralGovernance"]["maturationCurve"], device.days_in_vitro)
drift = compute_mahalanobis(device.profile_vector, expected)
if drift > artifact["policy"]["behavioralGovernance"]["dynamicDriftThreshold"]:
return pause("DRIFT_EXCEEDED")
# 7. Generate receipt + append to continuity chain
receipt = sign_receipt(artifact, workload, device)
if not append_to_chain(receipt):
return safe_mode("CHAIN_APPEND_FAILED") # fail-closed
return permit(receipt)
```

Response Categories

Response	Behavior	Recovery Path
halt	Workload rejected immediately. Signed rejection receipt generated. No computation occurs.	Resolve root cause; re-verify AGA artifact.
pause	Active workloads suspended. System awaits operator/donor action. No new workloads accepted.	Donor re-contact; new AGA with updated baseline.
safe_mode	All operations cease. Device enters minimal-function state. Chain gap marker appended.	Hardware inspection; re-provenance; new AGA.
permit	Computation proceeds. Signed receipt appended to continuity chain.	N/A (normal operation).

Table B.2. Response categories. All non-permit responses generate signed receipts.

Error Contract

Code	Trigger	Behavior
SEAL_INVALID	Signature verification fails	Halt; attest failure; reject workload
ARTIFACT_EXPIRED	Clock > expiry; no re-attestation	Halt; require donor reauthorization
DEVICE_MISMATCH	device.id ≠ artifact.subject.deviceId	Halt; provenance chain broken
SUBSTRATE_SWAP	Bio-PUF hash mismatch	Halt; physical investigation required
CATEGORY_PROHIBITED	Workload in prohibited list	Reject; log attempt
CATEGORY_NOT_PERMITTED	Workload not in permitted list	Reject (fail-closed on unlisted)
LATENCY_EXCEEDED	Crypto overhead > STDP budget	Halt; require FPGA acceleration
DRIFT_EXCEEDED	Mahalanobis > threshold × N epochs	Pause; donor re-contact
CHAIN_APPEND_FAILED	I/O error on receipt write	Safe mode (fail-closed)

Table B.1. Failure semantics. All non-PERMITTED outcomes generate signed receipts.

APPENDIX C

End-to-End Lifecycle

1. Donor Consent

Adult donor provides sample under consent specifying permitted categories, prohibited categories, MODERATE sensitivity ceiling, one-year term. Consent record signed ML-DSA-87; hash enters AGA artifact.

2. Tissue Provenance

Sample → iPSC → neurons. Each step attested ML-DSA-65. Chain-of-custody sealed; hash bound to consent.

3. Device Binding

Neurons cultured on MEA (Boundary 1). Bio-PUF baseline captured. AGA artifact created binding consent, provenance, protocol, Bio-PUF, and device ID. Signed ML-DSA-87.

4. Behavioral Baseline

Pre-workload profiling session. Multidimensional profile vector hashed into AGA behavioralBaselineHash.

5. Workload Request

Third-party submits pattern-recognition workload via cloud API. verify_aga_artifact() v8.0: seal → expiry → device+Bio-PUF → consent scope → STDP budget → dynamic drift → permitted.

6. Runtime

AGA active. Stimulation encrypted ML-KEM-768 (B2). Responses signed ML-DSA-44 (B3). Output signed ML-DSA-65 (B4), bound to full chain.

7. Receipt

ML-DSA-65 signed receipt appended to continuity chain. Attests artifact, device, category, timestamp, drift, result.

8. Audit

Auditor retrieves receipt, verifies signature, traces chain: output→response→stimulation→device→provenance→consent. Every link independently verifiable.

9. Donor Withdrawal

Donor exercises right to withdraw consent. AGA artifact immediately invalidated. System enters safe mode: all active workloads paused, no new workloads accepted. Proof of Withdrawal receipt generated and appended to continuity chain. Substrate proceeds to End-of-Life (Phase 11). Withdrawal is irrevocable—a new consent agreement requires a new AGA with a new chain. The continuity chain

from the withdrawn period is preserved for audit but marked terminated.

10. Drift Event

Month 8: attestation measures drift exceeding dynamicDriftThreshold for N consecutive intervals (hysteresis). System pauses. Donor contacted for consent reauthorization. New AGA issued with updated baseline and maturation curve.

11. End-of-Life

Viability drops below threshold (or donor withdrawal per Phase 9). Proof of Deprovisioning receipt generated: validated sterilization, no viable tissue remains, continuity chain terminated. ML-DSA-87 signed. AGA revoked.

APPENDIX D

Glossary

Term	Definition
AGA	Attested Governance Artifact. Sealed policy object enforced at runtime; also the broader framework for generating, enforcing, and verifying these artifacts.
Bio-PUF	Biologically-derived Physically Unclonable Function from spontaneous spiking topology.
CBOM	Cryptographic Bill of Materials (CycloneDX).
CL1	Cortical Labs biological computer (~200K neurons on MEA).
Consent Drift	Divergence between consent scope and evolved substrate capabilities.
Continuity Chain	Unbroken cryptographic chain: tissue→computation→output.
DIV	Days In Vitro. Duration since neural culture initialization on MEA.
FIPS 203 / 204	Federal Information Processing Standards for ML-KEM (203) and ML-DSA (204), published August 2024.
FRAND	Fair, Reasonable, Non-Discriminatory licensing.
iPSC	Induced Pluripotent Stem Cell.
MEA	Multi-Electrode Array.
Mahalanobis Distance	Multivariate statistical distance measuring deviation from a reference distribution, accounting for covariance. Used for drift detection.
ML-DSA	FIPS 204 PQC digital signature standard.
ML-KEM	FIPS 203 PQC key encapsulation standard.
OI	Organoid Intelligence. Field combining organoids with computing interfaces.
PQC	Post-Quantum Cryptography.
Proof of Deprovisioning	Signed receipt attesting biological substrate sterilization, no viable tissue remains, and continuity chain terminated.
STDP	Spike-Timing-Dependent Plasticity. Temporal constraint on neural learning feedback.

APPENDIX E

References

[1] Kagan BJ et al. "In vitro neurons learn and exhibit sentience..." Neuron 110:3952-69, 2022. DOI:10.1016/j.neuron.2022.09.001. PEER-REVIEWED.

[2] Cai H et al. "Brain organoid reservoir computing for AI." Nat Electron 6:1032-39, 2023. DOI:10.1038/s41928-023-01069-w. PEER-REVIEWED.

[3] Jordan FD et al. "Open and remotely accessible Neuroplatform for wetware computing." Front AI 7:1376042, 2024. DOI:10.3389/frai.2024.1376042. PEER-REVIEWED.

[4] Cortical Labs. "Living Human Brain Cells Play DOOM on a CL1." YouTube, Feb 25, 2026. PRIMARY: company demo with CTO/CSO narration.

[5] CL1 pricing (~$35K). cortical.io product page + Top Gear (Mar 2026). PRIMARY+SECONDARY.

[6] Brennan J. "Governance Gaps in Commercial Biocomputing: An Audit of Cortical Labs and FinalSpark." ResearchGate, 2025. AUTHOR-AFFILIATED. Findings independently verifiable from operators' public documentation.

[7] Raichle ME, Gusnard DA. "Appraising the brain's energy budget." PNAS 99(16):10237-39, 2002. DOI:10.1073/pnas.172399499. PEER-REVIEWED.

[8] NVIDIA. H100 Tensor Core GPU Datasheet, 2023. 700W TDP (SXM). PRIMARY: manufacturer.

[9] Gabriel E et al. "Human brain organoids assemble...bilateral optic vesicles." Cell Stem Cell 28(10):1740-57, 2021. DOI:10.1016/j.stem.2021.07.010. PEER-REVIEWED.

[10] Loh E, Loh W. "Playing Brains: Ethical Challenges Posed by Silicon Sentience and Hybrid Intelligence in DishBrain." PMC 10602981, 2023. PEER-REVIEWED.

[11] Skloot R. The Immortal Life of Henrietta Lacks. Crown, 2010.

[12] NIST FIPS 204: ML-DSA, Aug 2024. csrc.nist.gov/pubs/fips/204/final. PRIMARY.

[13] NIST FIPS 203: ML-KEM, Aug 2024. csrc.nist.gov/pubs/fips/203/final. PRIMARY.

[14] Hartung T et al. "The Baltimore Declaration toward the exploration of OI." Front Sci 1:1068159, 2023. DOI:10.3389/fsci.2023.1068159. PEER-REVIEWED.

[15] pqm4 project (github.com/mupq/pqm4). ARM Cortex-M4 PQC benchmarks for FIPS 204 (ML-DSA). PRIMARY.

[16] CycloneDX CBOM, OWASP, cyclonedx.org, 2024. PRIMARY.

[17] USPTO App 19/433,835. "Systems and Methods for Generating and Enforcing Attested Governance Artifacts." Filed Dec 2025. 20 claims. PRIMARY.

[18] Smirnova L et al. "Organoid intelligence (OI): the new frontier in biocomputing." Front Sci 1:1017235, 2023. DOI:10.3389/fsci.2023.1017235. PEER-REVIEWED.

[19] Attested Intelligence. NIST CAISI RFI Response, Mar 2026. PRIMARY.

[20] Attested Intelligence. NIST NCCoE RFI Response, Mar 2026. PRIMARY.

[21] Hartung T et al. "Brain organoids and OI from ethical, legal, and social points of view." Front AI 6:1307613, 2024. DOI:10.3389/frai.2023.1307613. PEER-REVIEWED.

[22] Yuste R et al. "Four ethical priorities for neurotechnologies and AI." Nature 551:159-63, 2017. DOI:10.1038/551159a. PEER-REVIEWED.

[23] Cortical Labs. Cortical Cloud API, cortical.io, Mar 2026. PRIMARY.

[24] Babbush R et al. Google Quantum AI, March 2026. 256-bit ECDLP breakable with ≤1,200 logical qubits, <500K physical qubits, ~9 min. PEER-REVIEWED.

[25] Attested Intelligence. AGA-PQC Reference Implementation: ML-DSA-65 Hybrid Composite Signatures. Internal benchmark, April 2026. AMD Ryzen 5 3550H, Go. AUTHOR-AFFILIATED.

CONFORMANCE CHECKLIST

M1 = MUST (all deployments) | **M2 = SHOULD** (multi-tenant/cloud) | **ADV = MAY** (operator discretion)

1. [M1] **Tissue Provenance** — Substrate bound to consent + differentiation protocol + Bio-PUF?
2. [M1] **Four-Boundary Attestation** — Signed records at all four boundaries?
3. [M1] **PQC Cryptography** — ML-DSA-65/ML-KEM-768 minimum, within STDP budget?
4. [M1] **Consent Scope** — Permitted/prohibited categories in sealed AGA artifact?
5. [M1] **Fail-Closed Enforcement** — Non-compliant computation blocked, not merely logged?
6. [M1] **Continuity Chain** — Unbroken chain tissue→output, including end-of-life termination?
7. [M2] **Bio-Compute CBOM** — Crypto dependencies inventoried including chemical profile?
8. [M2] **Dynamic Drift Monitoring** — Mahalanobis distance vs. maturation curve?
9. [M2] **Consent Expiry** — Artifact expires; donor reauthorization required?
10. [ADV] **(Optional) Substrate Monitoring** — Precautionary indicators + bioethics escalation?

Repo (planned): github.com/attested-intelligence/bio-compute-governance (CC-BY 4.0 + Apache 2.0)

Contact: Attested Intelligence Holdings LLC | attestedgovernance.com | neurocrypt.ai

---

WP-AIH-2026-001 | **v8.0** | **March 21, 2026** | Public | FRAND | CC-BY 4.0 + Apache 2.0 (schemas)