Ascend Dynamix — Patent Portfolio

Executive Overview

Ascend Dynamix LLC develops human-aligned, post-quantum security architectures that blend hybrid cryptography, biologically inspired design, and zero-trust principles. This portfolio summarizes three foundational provisional patent filings that define the AetherGuard™ BioCore and AetherPulse™ ecosystems.

Included Provisional Filings

• AetherGuard™ BioCore Security Platform (Application No. 63/893,463)
• Zero-Trust Mobile Network (ZTMN) (Application No. 63/901,270)
• Bio-Inspired Dual Post-Quantum Cybersecurity Architecture (Application No. 63/909,718)

This document is an executive summary for evaluators, accelerators, and potential partners. It is not a legal filing and should be read alongside the official USPTO documents.

1. AetherGuard™ BioCore Security Platform

Application No. 63/893,463 — Filed October 3, 2025

Summary

AetherGuard™ BioCore defines a hybrid post-quantum endpoint security architecture that combines ML-KEM, X25519, HKDF, and AES-GCM within a layered, self-healing runtime. The system is designed for home, enterprise, and field environments where downtime, coercion, and future cryptographic risk must be explicitly addressed.

Key Architectural Elements

• Hybrid PQC handshake: ML-KEM + X25519 with HKDF-derived symmetric keys.
• SAFE-Full runtime: integrity-checked, layered protection boundary.
• Dual-slot updates: zero-downtime deployment with health-gated rollback.
• Human-aligned controls: duress modes, decoy environments, and behavior-aware safeguards.

Primary Advantages

• Quantum-resistant key exchange without sacrificing performance.
• Reduced operational risk via atomic, health-gated updates.
• Improved coercion resistance through alternate-access and decoy scenarios.

2. Zero-Trust Mobile Network (ZTMN)

Application No. 63/901,270 — Filed October 17, 2025

Summary

The Zero-Trust Mobile Network (ZTMN) provisional patent covers a carrier-agnostic, data-only mobile communication framework that enables end-to-end encrypted signaling, media, and control between physical eSIM devices and virtual SIM environments. The architecture assumes untrusted transport and enforces identity-first, zero-trust policies across all layers.

Key Architectural Elements

- Virtual SIM to eSIM encrypted tunnels over data-only channels.
- Zero-trust access control aligned to identity and device posture.
- PQC-ready handshake pipeline integrated with AetherGuard™ BioCore.
- Reflexive routing and isolation behavior for compromised paths.

Primary Advantages

- Stronger privacy posture than traditional carrier-centric models.
- Flexible deployment across carriers, regions, and network types.
- Ready for future PQC mandates in mobile infrastructure.

3. Bio-Inspired Dual Post-Quantum Cybersecurity Architecture

Application No. 63/909,718 — Filed October 31, 2025

Summary

This provisional patent generalizes the AetherGuard™ and ZTMN design language into a bio-inspired, dual-PQC security fabric. It models encryption and system maintenance after DNA, enzymes, and neural tissue, combining two complementary post-quantum strands, autonomous maintenance agents, and a neural-style messaging mesh governed by distributed AI consensus.

Key Architectural Elements

• Dual-strand PQC: complementary encryption layers that validate and repair each other.
• Enzyme maintenance sub-layer: automatic integrity repair, entropy renewal, and mutation control.
• Neural communication mesh: node–synapse topology with reflex arcs and trust boundaries.
• AI governance: n-of-m consensus agents with immutable audit chains and decoy-state handling.

Primary Advantages

• Self-healing cryptographic infrastructure resilient to corruption and partial compromise.
• Enhanced resistance to coercion, insider threats, and replay analysis.
• Conceptual and practical foundation for future "living" security systems.

4. Strategic Context

Collectively, these three provisional patents define a cohesive vision for AetherGuard™ BioCore and AetherPulse™. They form the basis of an ecosystem that treats security as a living, adaptive process rather than a static control set. Ascend Dynamix positions these architectures for use in critical infrastructure, defense, secure AI, and high-integrity enterprise environments.

For detailed technical specifications, performance benchmarks, and integration discussions, Ascend Dynamix can provide extended briefs and reference implementations under appropriate review or NDA.