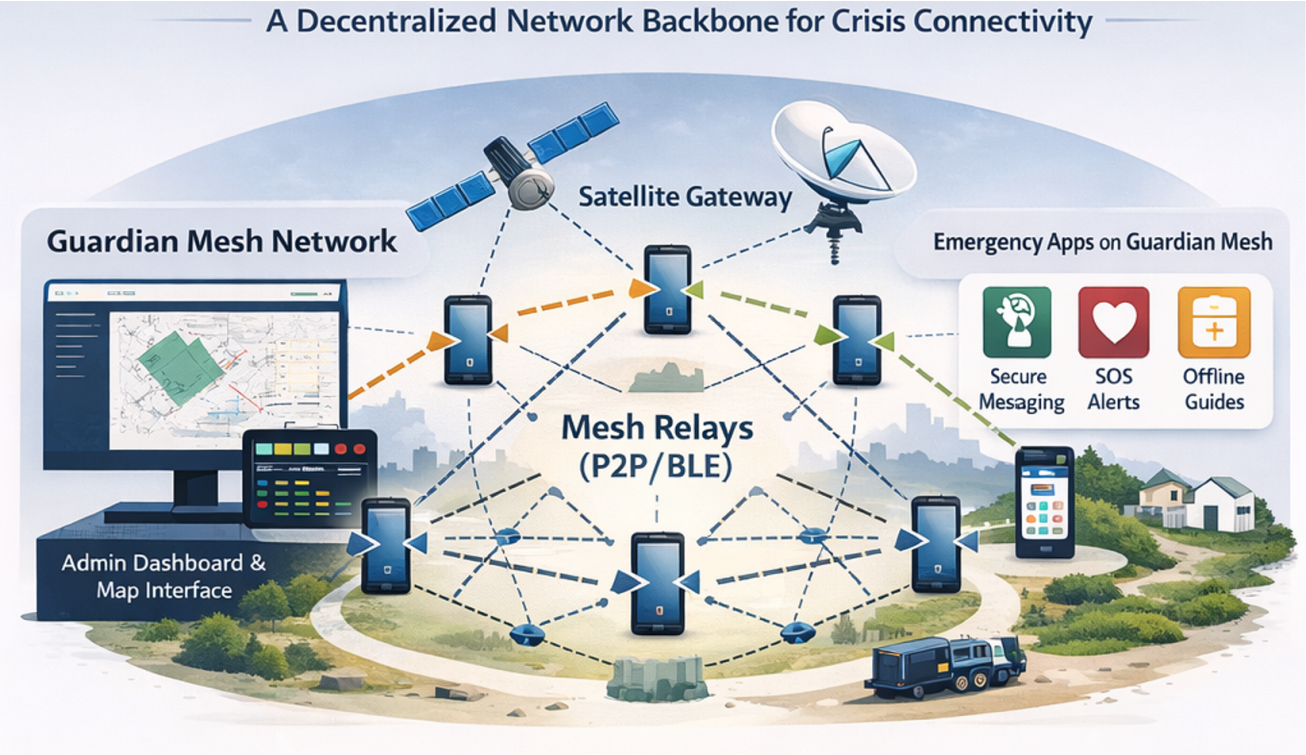
Guardian Mesh

Business Case — Resilient Decentralized Communication Infrastructure

“Communication that works when nothing else does.”



Guardian Mesh Inc.
Canadian Incorporated • NI 45-106 Compliant
March 2026 • Version 1.1

Confidential — For Authorized Recipients Only

Table of Contents

1 Executive Summary

Guardian Mesh is a **decentralized emergency communication platform** designed to operate reliably when traditional infrastructure fails. Combining a standalone cryptographic networking SDK, a decentralized relay network (Guardians), and a field-proven reference app (Ratchet), the platform delivers end-to-end encrypted messaging that works across seven transport types — including Bluetooth mesh and satellite links — with no central kill switch, no phone number registration, and full offline capability.

The platform addresses a critical gap: when natural disasters destroy cell towers, when remote communities lack coverage, and when censorship blocks conventional apps, people who most need to communicate are cut off. Guardian Mesh ensures they are not.

7	6-Layer	9,000+	12
Transport Types	Security Architecture	Automated Tests	Production Services

Guardian Mesh is **field-test ready** with over 9,000 automated tests across 525 test files, a completed security audit, live deployment infrastructure, and an enterprise backend supporting accounting, HR, AI-assisted administration, and a shareholder portal. The platform is **Canadian incorporated** and **NI 45-106 compliant**.

Key Value Proposition: Turn any app's users into relay nodes on a peer-to-peer network. Messages hop between devices via BLE mesh, Guardian relay nodes, and satellite/radio gateways. No central server. No registration. No kill switch.

2 Problem & Market Opportunity

The Problem

Communication infrastructure represents a critical vulnerability during crises. Natural disasters destroy cell towers, remote areas lack coverage entirely, and climate events increasingly disrupt connectivity. Existing messaging platforms, despite strong encryption, suffer from fundamental architectural limitations:

- **Centralized infrastructure** — A single company can be compelled to disable service or hand over metadata
- **Phone number requirements** — Identity tied to government-issued documents, excluding those without
- **Always-online assumption** — Messages fail when connectivity is intermittent or unavailable
- **App store dependency** — Distribution can be blocked regionally by platform gatekeepers
- **Metadata exposure** — Connection patterns reveal social graphs even with end-to-end encryption

Market Opportunity

Guardian Mesh addresses multiple large and growing markets:

Market Segment	Context	Drivers
Emergency Response	SAR, fire, police, disaster relief	Climate events increasing 3x since 1980s
Remote Communities	Rural, maritime, mining, exploration	3.7B people lack reliable connectivity
Humanitarian / NGO	Conflict zones, refugee operations	Growing need for censorship-resistant tools
Enterprise Security	Secure internal communications	Enterprise E2E encryption market growing rapidly
Journalism / Activism	Source protection, organizing	Press freedom declining in 70% of countries

Why Now: The convergence of increasing climate disasters, declining press freedom, growing enterprise security demands, and maturing BLE/mesh hardware creates a unique window. Existing solutions address fragments of the problem — Guardian Mesh is the first to unify mesh networking, delay-tolerant delivery, end-to-end encryption, and self-sovereign identity in a single, production-ready platform.

3 Solution Overview

Guardian Mesh is a three-part system: a standalone SDK for developers, a relay infrastructure backbone, and a privacy-first mobile app. Together, they form a decentralized communication network with no single point of failure.

Platform Architecture

RATCHET MOBILE APP	**End-to-end encrypted messaging • Safety alerts • Evidence capture • Emergency library • BLE mesh • Offline-first**
GUARDIAN MESH SDK	**Crypto (AES-256-GCM, X3DH, Double Ratchet) • Identity (Ed25519) • Transport (7 types) • DTN • Routing • Incentive**

Guardian Infrastructure	Relay nodes • WebSocket signaling • Noise XX federation • DHT discovery	**Enterprise Backend**	Admin • Accounting • HR • Shareholder portal • AI automation

Seven Transport Types

Guardian Mesh supports seven independent transport mechanisms, ensuring connectivity in any environment:

Transport	Range	Infrastructure	Best For
BLE Mesh	~100m per hop	None (peer-to-peer)	Offline, proximity
WebRTC	Global	STUN/TURN servers	Browser-to-browser
LAN / mDNS	Local network	None	Same building/campus
Guardian Relay	Global	Guardian nodes	Always-on backbone
Tor	Global	Tor network	Anonymity, censorship bypass
Satellite	Global	Iridium/Starlink	Remote/maritime areas
Sneakernet	Physical	None (QR/USB)	Air-gapped transfer

Messages automatically route through the best available transport, falling back through the cascade as options become unavailable. Delay-Tolerant Networking (DTN) bundles ensure messages are stored and forwarded even in intermittent connectivity, using epidemic routing with tiered Bloom filters for deduplication. Cross-cutting capabilities include packet-level traffic obfuscation with adaptive shaping and battery-aware cover traffic generation.

4 Technical Differentiation

Guardian Mesh introduces several novel technical contributions, backed by a comprehensive whitepaper targeting top-tier security conferences (USENIX Security, IEEE S&P;, ACM CCS):

Hop-Based TTL
Bundle lifetime measured in relay hops rather than wall-clock time, solving clock-skew challenges in disconnected networks where device clocks are unsynchronized.

Two-Stage Dead-Man Alerts
Soft warning to user's secondary devices before escalating to trusted contacts — dramatically reduces false positive emergency notifications while maintaining protection.

Network Witness Protocol
Multiple peers cryptographically acknowledge content hashes, providing tamper-proof provenance for evidence captured in the field. Prevents evidence suppression or fabrication.

Tiered Bloom Filters
Probabilistic duplicate detection for normal messages, exact-hash tracking for emergency bundles — critical messages are never incorrectly dropped.

Multi-Method Guardian Discovery
Cascading discovery (peer cache → DHT → DNS-over-HTTPS → hardcoded) provides resilience against multiple simultaneous blocking strategies.

Traffic Obfuscation & Cover Traffic
Packet-level obfuscation with constant-rate and adaptive traffic shaping makes Guardian relay traffic indistinguishable from background noise. Battery-aware cover traffic generation adapts to device state.

Gateway Hardware Integration
SatelliteGateway (Iridium/Starlink modems), RadioGateway (amateur/emergency radio), and DiasporaBridge provide hardware escape routes when all software transports are blocked.

Persistent Guardian Identity
Optional persistent registration preserves earned credits and reputation across offline periods. Encrypted key backup with PBKDF2 passphrase-based recovery. Emergency deregistration wipes all server-side traces for operators in hostile environments.

6-Layer Defense-in-Depth Architecture

Layer	Capability	Technology
1. Hybrid Mesh	Multiple transport paths	WebRTC, BLE, Tor, LAN, Satellite, Sneakernet
2. Self-Sovereign Identity	No registration authority	Ed25519 keys, SHA-256 identity hash
3. Distributed Storage	Resilient data persistence	Erasure coding, secure deletion
4. Metadata Resistance	Protect communication patterns	Onion routing, cover traffic, mixing
5. App Independence	No app store dependency	P2P APK distribution
6. Escape Routes	Last-resort connectivity	Satellite, radio, diaspora bridges

Cryptographic Foundation: Signal Protocol (X3DH + Double Ratchet) for pairwise messaging, MLS RFC 9420 for scalable group encryption, Ed25519 signing, X25519 key agreement, AES-256-GCM authenticated encryption — all implemented with audited *@noble/** libraries (zero-dependency, pure JavaScript).

5 Product Suite

Guardian Mesh SDK

Standalone npm package for third-party developers

Turn any app's users into relay nodes. 12 subpath exports covering crypto, identity, transport, protocol, DTN, gateway, guardian discovery, routing, incentive, storage, and MLS group messaging. Gateway subsystem provides SatelliteGateway, RadioGateway, and DiasporaBridge for hardware escape routes. Routing layer includes onion circuits, gossip-based peer discovery, and adaptive transport selection with dynamic path scoring. Traffic obfuscation with constant-rate and adaptive shaping. Battery-aware cover-traffic generation. Zero external dependencies in security paths. Published as **guardian-mesh-sdk** on npm.

Ratchet (Reference Implementation)

Field trial deployment — proves the SDK works on real devices

React Native + Expo SDK 55. Exercises every SDK capability in a real mobile environment: BLE mesh, guardian relay, E2E encryption, warrant canary, dead-man check-in, evidence capture with network witnesses, safety mapping, and offline emergency guides. Deployed in government field trials to validate the platform for procurement.

Guardian Infrastructure

Decentralized relay backbone

Always-on Guardian relay nodes with WebSocket signaling, Noise XX federation between guardians, store-and-forward message persistence, DHT-based peer discovery, onion routing for metadata resistance, and cover traffic generation. Optional persistent guardian registration preserves earned credits and reputation across offline periods with encrypted key backup and emergency deregistration for operators in hostile environments. Self-service guardian balance portal. Deployment via single-host installer, three-host rollout, Docker containers, or Raspberry Pi edge nodes.

Enterprise Backend

Full-featured business operations platform

Eight Python Flask servers: (1) Admin dashboard with IFRS accounting, HR management, and AI automation; (2) Guardian API with node directory, credits, revenue, and persistent registration; (3) Employee self-service portal; (4) Corporate shareholder portal (holdings, voting, dividends, KYC); (5) Investor subscription portal with Stripe payment processing, multi-tier investor classification, and KYC compliance; (6) Email service with templates, event bus, Celery async workers, and analytics; (7) Network visualization map; (8) Marketing site with guardian balance self-service. AI-assisted administration via Groq LLM with 46 endpoints across 7 domains: accounting (8), HR (7), corporate (6), revenue (3), fundraising (8), approval queue (4), and employee self-service (3). Fundraising AI includes grant discovery, sponsor matching, pitch optimization, and application drafting. Optional AI features — PII never sent to AI (47-field forbidden list with recursive verification).

SDK Integration Value: Any mobile or desktop app can integrate Guardian Mesh SDK to gain mesh relay capability. Each integrating app expands the relay network, creating a powerful network effect — more apps mean more relay nodes mean better coverage for everyone.

6 Revenue Model & Economics

Guardian Mesh generates revenue exclusively through **government emergency communications contracts** — powered by a decentralized guardian relay network that keeps infrastructure costs low and fully variable. The SDK is dual-licensed (AGPL-3.0 + commercial) and will be published after IP protections are filed. Non-dilutive grants (SR&ED;, IRAP, PacifiCan) supplement operating cash flow. Guardian relay operators are compensated as an operating cost from contract revenue.

Revenue Streams

Revenue Stream	Description	Y1 Target
Government Contracts	Municipal, provincial, and federal emergency communications pilots and deployments. Sole direct revenue strea	$25,000
Non-Dilutive Grants	SR&ED tax credits, IRAP, PacifiCan RDII — supplement cash flow, not primary revenue	$50K–$100K
Equity Investment	Seed round ($1.5M SAFE/convertible note) — primary capital source, 18-month runway	$1,500,000

Government Contract Tiers

Level	Example Agencies	Contract Type	Typical Value
Municipal	BC municipal emergency management	Pilot deployment	$50K–$100K / yr
Provincial	Emergency Management BC, Ontario EMO	Multi-year infrastructure	$100K–$250K / yr
Federal	Public Safety Canada, DND, Indigenous Services	Large-scale deployment	$250K–$1M+ / yr
International	UNHCR, Red Cross (future)	Humanitarian deployments	$100K–$500K

SDK Open-Source Model

The guardian-mesh-sdk is dual-licensed (AGPL-3.0 + commercial) and will be published after intellectual property protections are filed. Open-source adoption builds guardian relay network density and validates real-world deployment — both of which strengthen government contract sales. Commercial SDK licensing is a future revenue opportunity deferred to a later funding stage once network effects are established.

3-Year Revenue Forecast

Revenue Stream	Year 1	Year 2	Year 3
Government Contracts (sole revenue)	**$25,000**	**$450,000**	**$1,200,000**

Government revenue reflects realistic procurement timelines. Canadian government procurement cycles typically run 12–18 months for new vendors. Year 1 government revenue ($25K) assumes a pipeline conversation begins at funding close with a contract finalized in Q3–Q4 Y1 via Small Value Procurement or equivalent. Year 2 provincial contracts assume Standing Offer registration with PSPC initiated in Q1 Y1. Year 2 government total ($450K) includes the remaining $50K of the municipal pilot contract deferred from Y1.

The Guardian Credit Economy — Infrastructure Without Fixed Overhead. Revenue from all sources — government contracts, corporate sponsorships, licensing — is injected into monthly accounting periods. The company determines the credit price and total monthly payout pool based on available revenue. Guardians are paid via a 50/50 equal-plus-proportional settlement: half split equally among all active Guardians, half proportional to relay credits earned (Emergency=100, High=25, Normal=5, Low=2, Bulk=1). Guardian relay operators can optionally register persistently to preserve earned credits and reputation across offline periods, with encrypted key backup for identity recovery. In Year 2, ~200 Guardians earn ~$25/month each (~$60K/yr total COGS). This keeps infrastructure costs fully variable, scaling with revenue rather than against it.

7 Security & Compliance

Security is foundational to Guardian Mesh, not an afterthought. The platform implements defense-in-depth across every layer.

Cryptographic Foundation

Algorithm	Purpose	Standard
X3DH	Asynchronous key exchange	Signal Protocol
Double Ratchet	Per-message key derivation	Signal Protocol
MLS (TreeKEM)	Scalable group encryption	RFC 9420
AES-256-GCM	Authenticated encryption	NIST
Ed25519	Digital signatures, identity	EdDSA / RFC 8032
X25519	Key agreement	RFC 7748
HKDF-SHA256	Key derivation	RFC 5869

Privacy Protections

- **Self-sovereign identity** — No phone number, email, or registration. Users identified by SHA-256 hash of their Ed25519 public key.
- **Warrant canary** — Weekly Ed25519-signed statements confirming no legal compulsion received. Missing/expired canary triggers highest alarm.
- **Evidence tamper-proofing** — Photo/video signed with Ed25519, device anonymized with per-capture salt, location rounded to ~1km. Network witnesses provide distributed attestation.
- **Onion routing** — 3-hop circuits with cover traffic for metadata resistance.

- **AI PII firewall** — 47-field forbidden list with recursive deep verification. Regex scrubbing for emails, phone numbers, SIN/SSN. Only SHA-256 hashes stored in audit logs.

Enterprise Compliance

- **Canadian incorporated** with NI 45-106 compliance for securities offerings
- **IFRS-compatible accounting** with full chart of accounts, journal entries, ledger, budgets
- **JWT authentication** with TOTP 2FA, bcrypt hashing, account lockout, CSRF protection
- **AI approval workflow** — High-risk AI suggestions require human approval (7-day TTL auto-expiry)
- **Comprehensive audit trails** — All financial transactions, AI actions, and admin operations logged

Security Documentation

- **Formal threat model** — Comprehensive adversary analysis with mitigations for all identified attack vectors
- **Key lifecycle management** — Documented procedures for key generation, rotation, revocation, and secure deletion
- **4 Architectural Decision Records** — Cryptographic library selection, wire format, operational limitations formally documented
- **Security review scope** — Defined review boundaries and known issues tracking for continuous improvement

8 Production Readiness

Guardian Mesh has completed a comprehensive production readiness audit. All components score 10/10 on production readiness.

Component Readiness Scores

Component	Score	Tests	Status
Guardian Mesh SDK	10 / 10	81 tests, 6 suites	Field-Test Ready
Guardian API	10 / 10	4,565+ tests, 163 files	Field-Test Ready
Signaling Server	10 / 10	281 tests, 32 suites	Field-Test Ready
Ratchet Mobile	10 / 10	1,683 tests, 75 suites	Field-Test Ready
Admin Dashboard	10 / 10	2,106 Selenium + E2E tests	Production
Employee Portal	10 / 10	Full CRUD coverage	Production
Corporate Portal	10 / 10	Holdings, voting, dividends	Production
Guardian Web	10 / 10	SEO, SSR, balance checker	Production
Guardian Map	10 / 10	SPA with live data	Production

Test Coverage

Metric	Ratchet	Guardian Mesh	Threshold
Statements	83.6%	80.3%	≥ 82%
Branches	79.8%	65.3%	≥ 78%
Functions	85.3%	61.5%	≥ 72%
Lines	84.2%	82.8%	≥ 84%

Python Backend Testing

The Python Flask backend includes 525+ test files with 9,000+ test cases across 6 categories:

Category	Tests	Description
Static Analysis (tests/a/)	200+	Linting, code quality, no hardcoded secrets
Unit Tests (tests/u/)	901+	Isolated component, route, and repository tests
Integration Tests (tests/n/)	3,400+	End-to-end flows requiring MongoDB

Selenium Browser Tests	2,106	Full UI testing across all dashboards
E2E Playwright (specs/)	411+	Cross-service scenario and security tests
Ratchet + SDK (Jest)	2,045	1,683 mobile + 281 signaling + 81 SDK

Infrastructure

- **12 services** deployed across production infrastructure
- **Health check endpoints** on all servers with Prometheus-compatible metrics
- **Deployment options:** single-host installer, three-host rollout, Docker containers with Compose, Raspberry Pi edge nodes
- **Server automation:** systemd service definitions, Nginx reverse proxy, automated SSL/TLS and firewall scripts
- **Operations:** operator runbook, backup/restore procedures, rollback scripts, soak testing, reproducible builds
- **Security:** no hardcoded secrets (enforced by static analysis tests), environment-based configuration

CI/CD Pipeline

9 automated GitHub Actions workflows: code quality and linting, API telemetry validation, integration tests, Playwright E2E browser tests, smoke tests, multi-server matrix testing, Python backend matrix, public release builds, and pre-deployment sanity checks.

Documentation

- **Academic whitepaper** (44K words) targeting USENIX Security, IEEE S&P;, ACM CCS
- **IP inventory** — 34 innovations, 17 patentable, formally catalogued
- **Formal threat model** with adversary analysis and mitigations
- **4 Architectural Decision Records** documenting key technical decisions
- **11 SDK documentation guides** (crypto, identity, protocol, transport, DTN, gateway, guardian, routing, incentive, storage, MLS)
- **Developer Portal SPA** for third-party SDK integration
- **Operator runbook**, backup/restore guide, soak testing procedures, reproducible builds documentation

9 Roadmap & Next Steps

Guardian Mesh is production-ready today. The following milestones represent the path to full public launch:

Phase	Milestone	Status
Current	Field testing with early operator cohort	Active
Complete	Persistent guardian registration + key backup	Shipped
Complete	Guardian balance self-service portal	Shipped
Q2 2026	SDK published to npm for third-party developers	Ready
Q2 2026	Credit economy externalization (real payments)	Architecture complete
Q2 2026	Satellite/radio gateway hardware validation	Experimental
Q3 2026	App store launch (iOS + Android)	Configuration ready
Q3 2026	First enterprise SDK partnerships	Pipeline active
Q4 2026	Managed Guardian node hosting service	Planned
2027	Academic publication (security conferences)	Whitepaper ready

Network Effect Strategy

The SDK-first approach creates a powerful network effect: each app that integrates Guardian Mesh SDK adds relay nodes to the network, improving coverage for all participants. This means the network grows organically as developers adopt the SDK, without requiring Guardian Mesh to operate all relay infrastructure directly.

Defensibility

- **Technical moat** — Novel protocol innovations (5 published contributions), extensive cryptographic implementation
- **Network effects** — Each new relay node increases value for all participants
- **Open SDK, controlled infrastructure** — SDK is open for adoption; Guardian relay network is the monetizable backbone
- **Regulatory positioning** — Canadian incorporation, NI 45-106 compliance, IFRS accounting from day one

10 Investment Opportunity

Guardian Mesh Inc. is a Canadian incorporated company building production-ready, privacy-preserving decentralized communication infrastructure. The company is NI 45-106 compliant and operates a live investor portal with full shareholder services.

Why Invest in Guardian Mesh

- **Production-ready platform** — Not a whitepaper project — 9,000+ tests passing, 12 production services running, comprehensive security audit complete. The technology works today and is entering field testing.
- **Government contract revenue model** — Revenue comes exclusively from government emergency management contracts (municipal, provincial, federal). Large, recurring contracts with high LCV:CAC ratios once landed. Non-dilutive grants supplement cash flow.
- **Massive addressable market** — Emergency response, enterprise security, humanitarian operations, and privacy-conscious communications represent multi-billion dollar markets with growing demand.
- **Strong network effects** — SDK-first strategy means every integrating app expands the relay network. More nodes = better coverage = more adoption = more nodes.
- **Technical differentiation** — Five novel protocol contributions, academic whitepaper targeting top-tier venues. Deep technical moat that is difficult to replicate.
- **Regulatory readiness** — Canadian incorporation, NI 45-106 compliance, IFRS accounting, KYC integration, and comprehensive audit trails from day one.

Shareholder Services

The Guardian Mesh corporate portal provides comprehensive shareholder services:

- Real-time holdings and portfolio tracking
- Shareholder voting on corporate resolutions
- Dividend distributions and reinvestment preferences
- KYC compliance self-service
- Share transfers and secondary offerings
- Digital share certificates
- Virtual annual meeting attendance

Contact: For investment inquiries, visit the Guardian Mesh Investment Portal or contact the Guardian Mesh team. All offerings are subject to applicable securities regulations.

11 Investment to Date

Guardian Mesh has been built on a foundation of extraordinary founder commitment. Before a single external dollar was raised, the founder invested full-time engineering effort equivalent to a senior engineering team — producing a production-ready, security-audited platform that most funded startups take years to reach. The figures below demonstrate technical execution and founder conviction; company valuation is forward-looking and determined through investor discussions based on revenue potential, not cost-basis.

Sweat Equity

Contributor	Period	Schedule	Rate	Value
Bruce deGrosbois	2 years	52 wks × 6 days × 10 hrs	$100/hr	$624,000

Rate of $100/hr reflects market rate for senior full-stack / cryptographic engineering.

Cash Investment

Investor	Amount
Bruce deGrosbois	$15,000
Wendy Wilkins	$2,000
Michelle Corbett	$2,500
Total Cash	**$19,500**

Total Investment

Category	Amount
Sweat Equity	$624,000
Cash Investment	$19,500
Grand Total	**$643,500**

What the Investment Produced

Deliverable	Detail
Production codebase	182,000+ lines of code
Automated test suite	9,000+ tests across 525 files
Novel IP innovations	34 identified, 17 patentable

Production servers	12 services deployed
SDK	12 subpath exports, npm-ready
Mobile app	iOS + Android via Expo
Enterprise backend	Accounting, HR, corporate portal, AI automation
Security audit	6-layer defense-in-depth, formal threat model
Whitepaper	Academic-quality, targeting top-tier venues
Federal incorporation	CBCA Corp #1775511-2

$643,500 in founder commitment and direct cash ($624,000 sweat equity + $19,500 cash) — proof of technical execution prior to external capital. This produced a production-ready, security-audited platform with 34 novel IP innovations — 17 patentable. Valuation is based on forward revenue potential, not cost-basis.

Key Person Risk — Mitigation: The platform was built by a single founder. Mitigations: (1) comprehensive documentation for all protocols and architecture decisions; (2) 9,000+ automated tests as executable specification — any engineer can understand system behaviour by running tests; (3) clean modular architecture with explicit interfaces; (4) **90-day first-hire commitment** — committed first technical hire within 90 days of funding close; (5) **active co-founder search** underway as a pre-closing priority.

Guardian Mesh

Resilient. Decentralized. Private.

Guardian Mesh is building communication infrastructure that cannot be silenced, surveilled, or shut down. With a production-ready platform, novel technical innovations, and a sustainable economic model, Guardian Mesh is positioned to become the backbone of resilient communication worldwide.

7 Transport Types	**6-Layer Security**	**9,000+ Tests**
Ed25519 Identity	**Signal Protocol E2E**	**MLS Group Encryption**
12 Production Services	**46 AI Endpoints**	**5 Novel Contributions**

Guardian Mesh Inc. • Canadian Incorporated • NI 45-106 Compliant

This document is confidential and intended for authorized recipients only.