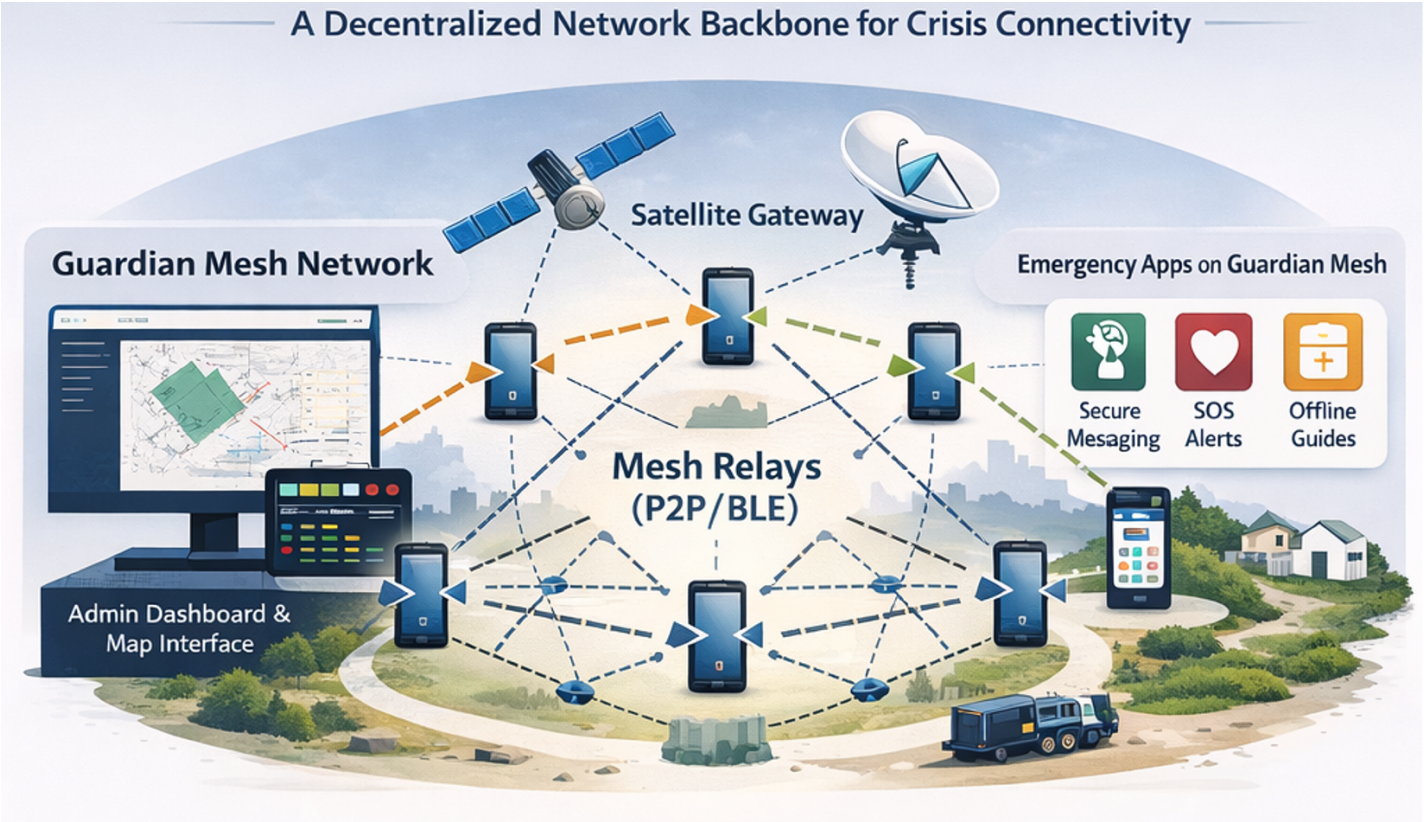
guardianmesh

Business Plan

Communication that works when nothing else does.



guardianmesh Inc. • Corporation No. 1775511-2
Federally Incorporated under CBCA • Victoria, BC
March 2026 • Version 1.1

CONFIDENTIAL

Important Notices

Forward-Looking Statements. This business plan contains forward-looking statements and projections based on assumptions and estimates made by guardianmesh Inc. management. These statements involve known and unknown risks, uncertainties, and other factors that may cause actual results, performance, or achievements to be materially different from those expressed or implied. Forward-looking statements include, but are not limited to, statements about projected revenues, market opportunities, product development timelines, and funding objectives. Readers are cautioned not to place undue reliance on these statements. guardianmesh Inc. undertakes no obligation to update or revise any forward-looking statements to reflect new information, future events, or changed circumstances.

Securities Notice (NI 45-106). guardianmesh Inc. is a corporation incorporated under the Canada Business Corporations Act (CBCA), Corporation No. 1775511-2. Any offering of securities by guardianmesh Inc. will comply with applicable Canadian securities legislation, including National Instrument 45-106 – Prospectus Exemptions and any applicable provincial securities laws in British Columbia and other relevant jurisdictions. This document does not constitute a prospectus or offering memorandum. Nothing herein shall be construed as a public offering of securities. Prospective investors should seek independent legal and financial advice.

Confidentiality. This document is strictly confidential and has been prepared solely for the use of the intended recipient. By receiving this document, the recipient agrees to treat all information contained herein as confidential and proprietary to guardianmesh Inc. The recipient shall not reproduce, distribute, or disclose any portion of this document to any third party without the prior written consent of guardianmesh Inc. Upon request, this document and all copies must be returned or securely destroyed.

This document does not constitute an offer to sell or a solicitation of an offer to buy any securities in any jurisdiction. No representation or warranty, express or implied, is made as to the accuracy, completeness, or fairness of the information and opinions contained in this document. guardianmesh Inc. and its directors, officers, employees, and advisors accept no liability whatsoever for any loss arising from any use of this document or its contents. All financial projections are illustrative only and are subject to change without notice.

guardianmesh Inc. • Corporation No. 1775511-2 • CBCA

Table of Contents

Part I: The Opportunity 6
1. Problem Statement 7
2. Market Opportunity 8
3. Competitive Landscape 9

Part II: The Solution 11
4. Product Suite 12
5. Technical Architecture 13
6. IP Portfolio 14
7. Security & Privacy 17
8. Production Readiness 18

Part III: Business Model & Financials 20
9. Revenue Model 21
10. Pricing Strategy 21
11. Go-to-Market Strategy 22
12. Financial Projections 23
13. Unit Economics 25

Part IV: Funding Strategy 27
14. Investment to Date 28
15. Government Grants & Contracts Strategy 29
16. Angel & VC Strategy 31
17. Use of Funds 32

Part V: Team & Execution 34
18. Team & Hiring 34
19. Roadmap & Milestones 35
20. Risk Analysis 37

Appendices
A. Codebase Metrics 37
B. IP Innovation Catalog 38
C. Grant Program Details 41
D. Financial Assumptions 43

ES Executive Summary

guardianmesh Inc. (Corporation No. 1775511-2, CBCA) is a federally incorporated Canadian company headquartered in Victoria, British Columbia, building a decentralized emergency communication platform designed to operate when traditional infrastructure fails. Founded by Bruce deGrosbois—a developer with 25 years of experience who launched his first platform in 2002—the company has completed two years of intensive, full-time development at a pace of 10 hours per day, six days per week. This sustained commitment has produced over 182,000 lines of production-ready code, 9,000+ passing automated tests, and 34 novel intellectual property innovations spanning cryptography, distributed networking, and secure communication protocols. guardianmesh Inc. is pre-revenue and production-ready. There are currently no signed contracts or active LOIs; government pipeline engagement begins at funding close. The seed round funds the transition from technical completion to first paid contract.

7	182K+	9,000+	34	$19.5K
Transport Types	Lines of Code	Passing Tests	IP Innovations	Cash Invested

The Opportunity

3.7 billion people worldwide lack access to reliable connectivity, leaving entire communities cut off during emergencies when they need communication most. Critical infrastructure—power grids, cellular towers, internet exchange points—remains a single point of failure during natural disasters, conflict, and state-directed shutdowns. Press freedom is in measurable decline in over 70% of countries globally, creating urgent demand for censorship-resistant communication tools. Simultaneously, the enterprise end-to-end encryption market is expanding rapidly as organizations recognize the legal, reputational, and operational risks of unprotected communications. guardianmesh addresses all four of these converging forces with a single, unified technical platform.

The Solution

guardianmesh is a deployable crisis-connectivity infrastructure platform with a licensable SDK and defensible IP. The core product is the Guardian Mesh SDK (a standalone cryptographic networking toolkit) and the GuardianMesh relay network (decentralized infrastructure backbone). Ratchet is the working reference app that proves the SDK runs on real devices in field conditions — it is not the product. The platform supports seven independent transport types—BLE mesh, WebRTC, LAN/mDNS, Guardian relay, Tor, satellite, and sneakernet—enabling communication across any available medium, including no internet at all. Security is implemented in six layers, incorporating the Signal Protocol (X3DH + Double Ratchet), MLS RFC 9420 group messaging, Noise XX federation, Ed25519 identity, AES-256-GCM encryption, and onion routing. Every cryptographic primitive is auditable, with zero reliance on closed-source dependencies.

The Ask

guardianmesh Inc. is raising a $1,500,000 CAD seed round to fund 24 months of runway covering core engineering hires, intellectual property protection (patent filing and trademark registration), and initial go-to-market execution: Victoria SAR field trial, government procurement registration, and SDK publication. The company's founder has already invested $19,500 CAD in direct cash expenses and committed $624,000 in sweat equity — demonstrating technical execution and founder conviction. Pre-money valuation is determined through investor discussions based on forward revenue potential, not cost-basis. The company currently has zero paying customers; the seed round's primary success metric is first paid contract — validating the platform commercially.

Revenue Projections: Year 1: $25,000 (partial-year government pilot) • Year 2: $450,000 (provincial + expanded municipal contracts) • Year 3: $1,200,000 (federal + provincial scale). Government revenue reflects realistic 12–18 month procurement cycles; Year 1 assumes pipeline conversations begin at funding close.

PART I

The Opportunity

The world's communication infrastructure is fragile — built for ideal conditions, not for the crises and communities that need it most. GuardianMesh addresses a fundamental gap: the absence of a resilient, privacy-preserving, incentivized mesh communication layer that works when everything else fails.

1 Problem Statement

Modern communication is critically dependent on centralized infrastructure that fails precisely when people need it most. When disasters destroy cell towers, entire regions lose the ability to coordinate emergency response. When remote communities lack coverage, they remain invisible to the digital economy and emergency services alike. When authoritarian regimes or corporate intermediaries block conventional apps, journalists, activists, and ordinary citizens lose their voice. The underlying assumption — that a functioning internet or cellular network is always available — is demonstrably false for billions of people worldwide.

Five Core Structural Problems

Centralized Infrastructure Dependency: All major messaging platforms require cellular or internet connectivity routed through centralized servers, creating single points of failure during natural disasters, power outages, and network outages.

Phone Number Requirements: Linking identity to phone numbers ties users to telecom providers, exposes real identities to carriers and governments, and excludes populations without phone numbers — including children, the undocumented, and those in regions with limited SIM access.

Always-Online Assumption: Existing secure messaging apps are designed exclusively for online use. None provide meaningful offline-first functionality with store-and-forward relay, multi-hop routing, or graceful degradation across heterogeneous transport layers.

App Store Dependency: Distribution through Apple App Store and Google Play Store creates censorship chokepoints. Governments have compelled removal of apps (e.g., VPNs, Telegram in Russia) and app stores require accounts linked to real identities.

Metadata Exposure: Even end-to-end encrypted applications leak substantial metadata: who communicates with whom, when, how frequently, and from where. This metadata is often more valuable to adversaries than message content.

Why Existing Solutions Fall Short

Solution	Offline	Multi-Transport	No Phone #	Incentives	Open Source	Decentral- ized
Signal	✗	✗	✗	✗	✓	✗
Briar	✓[1]	✗	✓	✗	✓	✓
Bridgefy	✓[2]	✗	✓	✗	✗	✗
goTenna	✓	✗	✓	✗	✗	✗
Meshtastic	✓	✗[3]	✓	✗	✓	✓
Helium	✗	✗	✗	✓	✓	✓
GuardianMesh	✓	✓	✓	✓	✓	✓

[1] BLE and WiFi Direct only — no LoRa, satellite, or internet transport.
[2] BLE only — highly range-limited, no multi-hop relay.
[3] LoRa only — requires dedicated hardware dongle.

GuardianMesh scores highest on architectural breadth and government/enterprise feature depth. Competitors have meaningful strengths this table does not fully capture: Signal has 40M+ active users and deep institutional trust; Meshtastic has an established hardware community and real-world deployments; Briar is trusted by activist and journalist communities. GuardianMesh's differentiation is the unified platform approach — brand

recognition and adoption must be earned through market execution.

2 Market Opportunity

The global demand for resilient, privacy-preserving communication is accelerating across multiple high-value sectors. GuardianMesh addresses a large and underserved market at the intersection of emergency preparedness, enterprise security, and decentralized infrastructure.

Total Addressable Market

$15B	$2B	$50M
TAM — Global Gov Crisis Infrastructure	SAM — Gov Agencies DDIL Communications	SOM — Year 3 Serviceable Market

SOM represents the Canadian government emergency management segment GuardianMesh is positioned to service by Year 3. Year 3 projected revenue of $1.2M represents ~3.9% initial capture of the SOM — consistent with early-stage market penetration.

Key Market Segments

Segment	Context	Growth Drivers
Emergency Response	Fire, flood, earthquake, and hurricane response teams lose cellular infrastructure exactly when coordination is most critical. FEMA, Red Cross, and municipal agencies require offline-capable, interoperable comms.	Climate disasters up 3x since 1980s; FEMA budget for comms resilience growing 18% YoY; Maui 2023 and Hurricane Ian exposed catastrophic gaps.
Remote Communities	3.7 billion people lack reliable internet access. Indigenous communities, rural areas, island nations, and developing regions need communication infrastructure that doesn't depend on telco investment.	UN Sustainable Development Goals; rising demand for digital inclusion; satellite costs declining but last-mile gap persists; community mesh deployments growing in Latin America and Southeast Asia.
Humanitarian & NGO	MSF, ICRC, and 50,000+ NGOs operating in conflict zones and disaster areas require communications that function under adversarial network conditions and cannot be intercepted by hostile state actors.	Conflict zones in Ukraine, Sudan, and Myanmar demonstrated the need; donor mandates for secure comms increasing; Signal blocked in multiple jurisdictions.
Enterprise Security	Fortune 500 companies, financial institutions, and critical infrastructure operators require zero-trust communications that cannot be surveilled by cloud providers or intercepted during network outages.	Zero-trust adoption growing 17% CAGR; SEC cyber disclosure rules; supply chain attack awareness post-SolarWinds; enterprise demand for self-hosted secure comms.
Journalism & Activism	130+ journalists imprisoned annually; press freedom declining in 70% of countries. Investigative journalists, whistleblowers, and civil society organizations require metadata-resistant, censorship-proof communication.	CPJ and RSF reporting record journalist arrests; Pegasus spyware revelations; Freedom of the Press Foundation partnerships; Signal blocked in Iran, Russia, China.
Defence & Intelligence	Military units, intelligence agencies, and national security contractors require OPSEC-grade communications that function in denied, degraded, and intermittent environments (DDIL) without reliance on adversary-controlled infrastructure.	NATO DDIL communication requirements; US DoD Modernization priorities; DARPA mesh networking programs; lessons from Ukraine battlefield communications.
IoT & Industrial	Industrial IoT deployments in mining, offshore energy, agriculture, and logistics require secure device-to-device messaging without continuous cloud connectivity. 15.1 billion connected devices by 2030.	Industry 4.0 automation; edge computing adoption; OT/IT convergence security; LoRa and BLE 5.0 hardware maturation enabling low-power mesh networking at scale.

Why Now: Five macro-forces are converging to create an ideal market entry window. (1) **Climate disasters** have increased 3x since the 1980s, exposing critical gaps in emergency communication infrastructure. (2) **Declining press freedom** in 70% of countries creates urgent demand for censorship-resistant tools. (3) **BLE 5.0 hardware maturation** has made low-power mesh networking viable on commodity smartphones without custom hardware. (4) **Post-Snowden privacy awareness** has fundamentally shifted enterprise and government procurement toward zero-trust, metadata-resistant solutions. (5) **Enterprise zero-trust adoption** growing at 17% CAGR is expanding the buyer universe beyond traditional security-conscious niches into mainstream enterprise.

3 Competitive Landscape

GuardianMesh occupies a unique position in the secure communications landscape — the only solution combining multi-transport offline resilience, self-sovereign identity, cryptographic relay incentives, and open-source auditability in a single platform.

Feature Comparison: GuardianMesh vs. Alternatives

Solution	Transport Types	Offline Capable	Relay Incentives	Identity Model	Hardware Required	E2E Encryption
GuardianMesh	7 (BLE Mesh, WebRTC, LAN, Guardian Relay, Tor, Satellite, Sneakernet)	Yes	Credit economy (relay receipts)	Self-sovereign (Ed25519)	No	Signal Protocol + MLS RFC 9420
Signal	1 (internet)	No	None	Phone number	No	Signal Protocol
Briar	2 (BLE + WiFi Direct)	Partial	None	Username (Bramble ID)	No	Bramble Protocol
Bridgefy	1 (BLE)	Yes	None	Device ID	No	Proprietary (E2E added later)
goTenna	1 (radio ASKOS band)	Yes	None	Device ID	Yes ($179+)	Proprietary (AES-256)
Meshtastic	1 (LoRa)	Yes	None	Device ID	Yes ($30+)	AES-256

Defensibility: Moat Analysis

GuardianMesh's competitive position is reinforced by four compounding moats that become stronger as adoption grows:

Technical Moat: The GuardianMesh SDK embodies 34 distinct IP innovations across cryptographic protocol design, multi-transport routing, and incentive mechanisms — representing years of R&D; that competitors cannot replicate quickly. The 182,000+ lines of production code span 7 transport layers with formal protocol specifications.

Network Effects: SDK adoption by third-party developers directly grows the relay network — every new app built on GuardianMesh adds relay capacity. This creates a virtuous cycle: more relays improve coverage, attracting more users, attracting more developers, deploying more relays. This flywheel is absent from all competing solutions.

Dual-License Revenue Model: The AGPL open-source license enables community adoption and security auditing while the commercial license creates a revenue moat for enterprise and government customers who cannot operate under AGPL. This bifurcation prevents competitors from simply forking and commercializing the codebase.

First-Mover in Incentivized Mesh: No existing mesh communication solution includes a cryptographic credit economy for relay operators. GuardianMesh establishes the standard protocol (relay receipts, settlement algorithm, payout rails) before any competitor has entered this space — creating protocol-level lock-in as the ecosystem develops.

PART II

The Solution

GuardianMesh is a vertically integrated communications platform built from first principles. Where Part I outlined the surveillance crisis and market opportunity, Part II details the technical solution: a production-ready SDK, decentralized relay network, and field-trial-ready reference deployment that together form a production-ready, privacy-preserving mesh communications stack with breadth of transport and security depth not currently matched by any single competing platform.

The platform spans 182,000+ lines of code, 9,000+ tests across 525 files, and 34 formally identified IP innovations — all developed by a single founder with 25 years of engineering experience, proving that focused expertise can out-execute large teams on deeply technical problems.

4 Product Suite

GuardianMesh is a layered infrastructure platform totalling 182,000+ lines of production code. The SDK and relay network are the revenue-generating core; Ratchet is the reference implementation that validates the platform in field conditions; the operations backend supports administration and investor services.

Product 1: guardian-mesh-sdk

A standalone npm package that will be published for third-party developers. The SDK provides the cryptographic and networking primitives needed to build any privacy-preserving mesh application — without requiring developers to understand the underlying protocols.

Scale: ~28,000 lines of code across 12 subpath exports

Exports: /crypto, /crypto/mls, /identity, /protocol, /transport, /dtn, /gateway, /guardian, /routing, /incentive, /storage — each independently importable

Security: Zero external dependencies in all security-critical paths; pure JS via @noble/* (audited, zero-dep)

Licensing: AGPL open-source + commercial dual license — open for community, paid for enterprise

Identity: Self-sovereign via SHA-256(Ed25519 public key) — no phone number, no email required

Protocol: Signal Protocol (X3DH + Double Ratchet) for pairwise; MLS RFC 9420 for group messaging

Product 2: Guardian Infrastructure

A field-test ready infrastructure backbone consisting of a TypeScript signaling server and a Python Flask backend with eight specialized services. Operators deploy this stack to run Guardian nodes and earn credit payouts for relaying traffic. Includes optional persistent guardian registration with encrypted key backup, self-service balance portal, and emergency deregistration for operators in hostile environments.

Component	Stack	Port	Function
Signaling Server	TypeScript / WebSocket	—	Guardian relay, Noise XX federation
Guardian API	Python Flask + SQLite	3002	Node directory, credits, revenue, persistent registration
Operations Backend (7 servers)	Python Flask + MongoDB	various	Admin, governance, investor services, email, web, map

Operations Backend: A full enterprise operations stack (accounting, HR, corporate governance, investor services) with AI-assisted administration. Detail in Appendix A.

Product 3: Ratchet (Reference Implementation)

Ratchet is the working proof that the SDK runs on real devices. It is not the product — it is the demonstration that the infrastructure works in field conditions. Built with React Native + Expo SDK 55, it exercises every SDK capability and provides a turnkey deployment for government field trials. Its role is to validate the platform for government buyers, not to acquire consumer users.

Messaging: E2E encrypted via X3DH + Double Ratchet; MLS for group chats

Transport: BLE mesh networking for fully offline, infrastructure-free communication

Safety: Warrant canary (weekly Ed25519-signed), dead-man check-in with two-stage alert
Evidence: Photo/video capture with Ed25519 signing and network witnesses for tamper-proof documentation
Safety Mapping: Incident reporting and real-time safety visualization
Library: Offline-first emergency guides — accessible with no connectivity
Architecture: Offline-first; functions without internet, cellular, or any central server

SDK Network Effect: Every third-party app built on guardian-mesh-sdk strengthens the Guardian node network. More apps → more relayed traffic → more guardian payouts → more nodes deployed → better coverage for all users. This creates a virtuous cycle where the SDK's open-source adoption directly monetizes the infrastructure business — a dynamic unavailable to single-product competitors.

5 Technical Architecture

GuardianMesh is architected as a layered defense system. No single failure — technical, legal, or infrastructural — can compromise user privacy or disrupt communications. Each layer is independently designed and verified.

7 Transport Types

The SDK implements seven distinct transport mechanisms, enabling communication across any physical environment. The adaptive transport scorer selects the optimal path based on latency, reliability, and censorship risk.

Transport	Medium	Range	Infrastructure	Use Case
BLE Mesh	Bluetooth LE	~100 m/hop	None (peer-to-peer)	Offline proximity; no infrastructure required
WebRTC	Internet	Global	STUN/TURN servers	Browser-to-browser real-time communication
LAN / mDNS	Ethernet/Wi-Fi	Local network	None	Same building or campus; no infrastructure
Guardian Relay	Internet	Global	Guardian nodes	Always-on backbone; persistent relay network
Tor	Internet	Global	Tor network	Anonymity and censorship bypass
Satellite	Satellite RF	Global	Iridium/Starlink	Remote and maritime areas; no ground infrastructure
Sneakernet	Physical (QR/USB)	Physical	None	Air-gapped transfer; extreme network denial

6-Layer Defense-in-Depth

Privacy is not a feature — it is the architecture. Six independent defensive layers ensure that even a complete compromise of any single layer cannot expose user data or disrupt service.

Layer	Name	Mechanism	Threat Defeated
1	Hybrid Mesh	7 transports with adaptive scoring; epidemic routing with hop-based TTL	Network takedown, ISP blocking, infrastructure seizure

Layer	Name	Mechanism	Threat Defeated
2	Self-Sovereign Identity	SHA-256(Ed25519 pubkey); no phone/email registration	Identity correlation, subpoena for subscriber records
3	Distributed Storage	Reed-Solomon erasure coding (WASM); secure deletion; no central message store	Server seizure, data retention orders
4	Metadata Resistance	3-hop onion routing with cover traffic; mixing	Traffic analysis, timing correlation attacks
5	App Independence	P2P APK distribution via mesh; no app store dependency	Platform bans, app store removal, vendor lock-in
6	Escape Routes	Satellite, radio, diaspora gateways; sneakernet transport	Total internet shutdown, extreme censorship scenarios

Cryptographic Foundation

All cryptographic primitives are implemented via the @noble/* library family — pure JavaScript, zero external dependencies, independently audited. This eliminates supply-chain risk from native crypto bindings and ensures the same security guarantees across all platforms.

X3DH (Extended Triple Diffie-Hellman): Asynchronous key exchange (Signal Protocol); enables secure messaging to offline recipients

Double Ratchet Algorithm: Per-message key derivation with forward secrecy and break-in recovery for all pairwise messaging (Signal Protocol)

MLS RFC 9420 (TreeKEM): Scalable group encryption with O(log n) key operations per member update; standardized by IETF

Ed25519: Digital signing for identity proofs, warrant canaries, evidence attestation, and relay receipts

X25519: Elliptic curve Diffie-Hellman key agreement; basis for all ephemeral session keys

AES-256-GCM: Authenticated encryption for all stored data and secure enclave operations

HKDF-SHA256: Key derivation for ratchet steps, session keys, and bundle encryption

Delay-Tolerant Networking (DTN)

GuardianMesh implements epidemic routing with two proprietary innovations that constitute separate IP filings. Messages are wrapped in DTN bundles and propagated through the network even in the absence of end-to-end connectivity.

Hop-Based TTL (IP-001): Message lifetime measured in relay hops rather than wall-clock time, eliminating sensitivity to clock skew across disconnected network segments. Directly applicable to military, space, and IoT DTN deployments.

Tiered Bloom Filters (IP-002): Multi-tier probabilistic deduplication with a mathematical guarantee of zero false positives for emergency-priority messages — critical when a missed message could cost a life.

Epidemic Router: Probabilistic message spreading with controlled fanout; adapts to network density and link quality in real time.

6 IP Portfolio

A formal IP audit identified 34 innovations across 7 categories. These innovations represent independent, defensible intellectual property — not incremental improvements to existing art. The portfolio has been structured to support both patent filings and trade secret protection depending on disclosure risk.

34 innovations · 7 categories · AccelerateIP-eligible · SR&ED-eligible; R&D;

Complete IP Innovation Register

ID	Innovation Name	Category	IP Type	Priority
IP-001	Hop-Based TTL for DTN	Algorithm	Patentable	**Critical**
IP-002	Tiered Bloom Filters with Emergency Bypass	Algorithm	Patentable	**Critical**
IP-003	Two-Stage Dead-Man Alert	Algorithm	Patentable	**Critical**
IP-004	Network Witness Protocol	Algorithm	Patentable	**Critical**
IP-005	Adaptive Battery-Aware Cover Traffic	Algorithm	Patentable	**High**
IP-006	Multi-Method Cascading Discovery	Algorithm	Patentable	**High**
IP-007	Earned-Only Credit System	Economic	Trade Secret	**High**
IP-008	50/50 Equal + Proportional Settlement	Economic	Patentable	**Critical**
IP-009	Credit Account Persistence via HKDF	Economic	Patentable	**High**
IP-010	Relay Diversity Weight	Economic	Trade Secret	**Medium**
IP-011	Priority-Weighted Credits with Federation Multiplier	Economic	Trade Secret	**Medium**
IP-012	Duress PIN with Decoy Account	Security	Patentable	**High**
IP-013	Ed25519-Only Authentication	Security	Trade Secret	**Medium**
IP-014	5-Level Web-of-Trust	Security	Patentable	**High**
IP-015	Noise XX Handshake with DPI-Resistant Key Exchange	Security	Patentable	**High**
IP-016	Warrant Canary System	Security	Copyright	**Medium**
IP-017	APK Transparency Log	Security	Patentable	**Medium**
IP-018	Guardian Mesh Federation Protocol	Architecture	Trade Secret	**High**
IP-019	Online Logistic Regression Peer Scorer	Architecture	Patentable	**High**
IP-020	Composite Guardian Health Score	Architecture	Trade Secret	**Medium**
IP-021	Context-Aware Transport Selection	Architecture	Patentable	**Medium**
IP-022	Onion Routing for Mobile DTN	Architecture	Copyright	**Medium**
IP-023	Reed-Solomon Erasure Coding (WASM)	Architecture	Copyright	**Medium**
IP-024	Secure Deletion via Partition Key Rotation	Architecture	Trade Secret	**Medium**
IP-025	Sneakernet Transport (QR + File)	Infrastructure	Patentable	**Medium**
IP-026	Satellite/Radio Gateway	Infrastructure	Copyright	**Medium**
IP-027	Diaspora Bridge	Infrastructure	Patentable	**Medium**

ID	Innovation Name	Category	IP Type	Priority
IP-028	P2P APK Distribution via Mesh	Infrastructure	Patentable	**Medium**
IP-029	BLE Peripheral Mode with GATT Server	Infrastructure	Trade Secret	**Medium**
IP-030	Traffic Obfuscation Layer	Infrastructure	Copyright	**Medium**
IP-031	Academic-Quality Whitepaper	Documentation	Copyright	**High**
IP-032	Comprehensive Threat Model	Documentation	Trade Secret	**Medium**
IP-033	Reproducible Builds System	Process	Copyright	**Medium**
IP-034	7-Day Soak Test Automation	Process	Trade Secret	**Low**

Top 6 High-Priority Innovations

The following six innovations have been identified as highest commercial value based on market breadth, licensing potential, and barriers to independent reinvention.

IP-001: Hop-Based TTL — Clock-Skew Resistant DTN Measures message lifetime in relay hops rather than wall-clock time, eliminating the primary failure mode of delay-tolerant networks in environments with no NTP synchronization. Commercial value: military communications, satellite mesh, deep-space relay, industrial IoT. No prior art identified for this specific approach.

IP-002: Tiered Bloom Filters — Zero False Positives for Emergency Messages A multi-tier probabilistic deduplication architecture with a mathematical guarantee that emergency-priority messages are never suppressed by a false positive. Standard Bloom filters cannot provide this guarantee. Commercial value: emergency services, disaster response networks, medical alert systems.

IP-003: Two-Stage Dead-Man Check-In — Reduced False Positive Alerts A staged alert protocol that issues a private warning before escalating to a public emergency alert, dramatically reducing alert fatigue in personal safety applications. Commercial value: lone worker safety, human rights defender tools, domestic violence protection applications.

IP-004: Network Witness — Distributed Evidence Attestation Multiple independent nodes sign the SHA-256 hash of captured evidence (NOT the content) using Ed25519, proving existence and integrity offline without exposing the evidence to witnesses. Creates a tamper-proof chain of custody without a trusted central authority. Commercial value: human rights documentation, legal proceedings, law enforcement body camera alternatives, insurance claims.

IP-008: 50/50 Settlement Algorithm — Fair Decentralized Revenue Split A relay revenue settlement formula that splits 50% equally among all participating operators and 50% proportionally to traffic relayed, balancing incentives for small and large operators. Commercial value: any decentralized network requiring operator revenue sharing — ISP mesh, community broadband, satellite ground station networks.

IP-006: Multi-Method Discovery — 7-Level Fallback Chain A guardian node discovery mechanism that cascades through seven independent methods in decentralization order — starting from zero-infrastructure methods (LAN/mDNS, BLE, peer cache) through decentralized infrastructure (DHT, DoH, session gossip) to hardcoded seeds as the last resort — before declaring discovery failure. Makes the network censorship-resistant by eliminating any single discoverable entry point. Commercial value: censorship-circumvention tools, enterprise zero-trust networks, crisis communications infrastructure.

Patent & Protection Strategy

AccelerateIP Program: GuardianMesh qualifies for CIPO's AccelerateIP program through the Venture Capital Catalyst Initiative, enabling faster prosecution of priority filings at reduced cost.

SR&ED; Eligibility: The R&D; activities underlying IP-001, IP-002, IP-003, IP-004, IP-006, and IP-008 constitute eligible SR&ED; expenditures under CRA guidelines, generating investment tax credits on development costs already incurred.

Trade Secret Protection: Innovations with high reverse-engineering difficulty (tiered Bloom filter parameters, settlement formula coefficients, onion routing topology) are maintained as trade secrets pending competitive analysis.

Dual Licensing: AGPL open-source for community adoption; commercial license for enterprise integrators who require proprietary embedding. The SDK's open-source release does not constitute prior art against novel method claims.

Defensive Publication: Low-priority innovations will be defensively published to prevent competitors from patenting obvious extensions of the GuardianMesh approach.

7 Security & Privacy

Security is not a layer applied to GuardianMesh — it is the substrate from which the platform is built. Every protocol choice, data model, and API design decision is evaluated against the threat model of a state-level adversary with full network visibility.

Cryptographic Algorithm Suite

Algorithm	Standard	Purpose	Key Size / Output
X3DH	Signal Protocol	Asynchronous key agreement (pairwise messaging)	X25519 ephemeral + identity keys
Double Ratchet	Signal Protocol	Forward secrecy + break-in recovery	32-byte chain keys, AES-256-GCM messages
MLS	RFC 9420 (IETF)	Scalable group key agreement	TreeKEM; O(log n) key operations
AES-256-GCM	NIST FIPS 197	Authenticated encryption (storage + enclave)	256-bit key, 96-bit nonce, 128-bit tag
Ed25519	RFC 8032	Digital signatures (identity, canary, evidence)	255-bit curve, 64-byte signature
X25519	RFC 7748	Elliptic curve DH key agreement	255-bit curve, 32-byte shared secret
HKDF-SHA256	RFC 5869	Key derivation (ratchet, sessions, bundles)	Variable output; 256-bit PRK

Privacy Protection Architecture

Self-Sovereign Identity: Users are identified solely by SHA-256(Ed25519 public key). No phone number, email address, government ID, or payment information is collected or required at any point.

Warrant Canary: Weekly Ed25519-signed canary statements are published with three severity levels: ok, warning, and critical. Statements become stale after 7 days and expired after 14 days; either condition triggers automatic client-side alerts. This provides legal protection without requiring the platform to actively notify users of secret orders.

Evidence Tamper-Proofing: Photos and videos captured in the Ratchet app are signed at capture time by the device's Ed25519 identity key. Device metadata is anonymized with a per-capture salt, and location is rounded to approximately 1 km to prevent precise tracking. Network witnesses — multiple independent nodes — sign the content hash (not the content itself), creating a chain of custody that is mathematically verifiable in court without a trusted intermediary.

Onion Routing: All relay traffic is wrapped in 3-hop onion routing with cover traffic injection. No single relay node can determine both the source and destination of a message. Cover traffic prevents traffic analysis even by a global passive adversary.

AI PII Firewall: The admin Groq AI integration enforces a 47-field forbidden list (FORBIDDEN_FIELDS frozenset) with recursive deep verification and regex scrubbing of phone numbers, email addresses, SIN numbers, SSNs, and other PII patterns. A _verify_no_forbidden_fields() check runs immediately before every API call. Only SHA-256 hashes appear in AI audit logs. All AI features are disabled by default (AI_ENABLED=false) and require explicit per-feature opt-in.

Duress PIN: Users can configure a duress PIN (stored as SHA-256 with domain separation "ratchet-duress-pin:") that, when entered, triggers an emergency wipe of real data and presents a decoy account with fabricated message history — protecting users under physical coercion.

Regulatory Compliance

GuardianMesh's privacy-by-design architecture exceeds the requirements of Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and is positioned for compliance with the forthcoming Consumer Privacy Protection Act (CPPA, Bill C-27). Key considerations:

Data minimization: No PII collected; identity hashes are not reversible to natural person identifiers without the original public key.

Purpose limitation: Message content is inaccessible to the platform operator by cryptographic construction — not policy.

Right to erasure: Because no PII is stored, erasure requests are satisfied by design. Users delete their local key material to effectively erase their identity.

Breach notification: A server compromise exposes only ciphertext and identity hashes — not names, contacts, or message content. Breach impact is materially limited.

Cross-border transfers: The decentralized architecture means data may transit nodes in multiple jurisdictions. All data in transit is encrypted end-to-end; relay nodes cannot read content.

8 Production Readiness

GuardianMesh is not a prototype. Every component listed below is in production-quality state: deployed, tested, and documented. The platform is ready for government field trials and operator onboarding without requiring additional development work.

Component Readiness

Component	Status	Evidence
guardian-mesh-sdk	Pilot-Ready	81 tests, 6 suites; all crypto verified
Guardian API	Pilot-Ready	4,565 tests; SQLite schema v8; persistent registration
Signaling Server	Pilot-Ready	281 tests; Noise XX federation tested
Ratchet (Reference App)	Pilot-Ready	1,683 tests, 75 suites; exercises full SDK
Operations Backend	Operator-Ready	Internally validated; 8 Flask servers running
Third-Party Security Audit	Planned	Budgeted in Legal/IP; post-funding priority

Automated Test Coverage

All coverage thresholds are enforced in CI. The platform has 9,000+ tests across 525 files, covering unit, integration, static analysis, and end-to-end scenarios.

Project	Statements	Branches	Functions	Lines	Suites / Tests
Ratchet (JS/TS)	83.6%	79.8%	85.3%	84.2%	75 suites / 1,683 tests
Guardian Mesh (JS/TS)	80.3%	65.3%	61.5%	82.8%	25 suites / 262 tests
Python Backend (static)	—	—	—	—	14 test files
Python Backend (unit)	—	—	—	—	21 test files
Python Backend (integration)	—	—	—	—	68 test files
Python Backend (e2e)	—	—	—	—	10 test files

Python backend: 113 test files total across four categories. Static analysis tests require no database and run in CI without infrastructure dependencies. Integration tests use MongoDB and verify end-to-end flows including AI approval queues, settlement calculations, and multi-server workflows.

Infrastructure & Deployment

Service count: 10+ independent services deployable as a coordinated stack or standalone components

Health checks: All Flask servers expose /health endpoints with Prometheus metrics; signaling server exposes WebSocket heartbeat; MongoDB and SQLite connections verified at startup

Deployment options: Single-host installer (rapid operator onboarding), three-host production rollout (HA configuration), and Docker Compose (development/CI) — all documented in the operator runbook

Operator runbook: Complete step-by-step setup, configuration, key rotation, backup/restore, rollback scripts, soak testing, and incident response procedures documented and validated

Environment configuration: All secrets and feature flags managed via .env files; no hardcoded credentials; AI features require explicit opt-in per feature flag

Database strategy: MongoDB for document-store workloads (admin, employee, corporate); SQLite for high-read relay accounting (guardian_api); no external dependencies for core relay functionality

Zero-downtime operations: Rolling updates supported; message delivery unaffected by single-node restarts due to DTN epidemic routing

PART III

Business Model & Financials

Part III presents the revenue architecture, pricing framework, go-to-market strategy, and three-year financial projections for guardianmesh Inc. Together these sections demonstrate a clear path from government pilot contracts to multi-year provincial and federal procurement. Enterprise licensing and SDK adoption are parallel upside opportunities, not primary revenue at this stage. The dominant strategy is: government-first now; enterprise and SDK monetization later or opportunistically alongside.

9 Revenue Model

guardianmesh generates revenue by providing resilient emergency communication infrastructure to government emergency management agencies. Enterprise revenue is a secondary future lane. Guardians — people who host relay nodes — are paid by the company for providing network capacity; they are a cost center, not a revenue source. Revenue comes from organizations that need the network to work when nothing else does.

1. Government Emergency Infrastructure Contracts (Primary)

When internet and cellular infrastructure fail — during wildfires, ice storms, earthquakes, or grid outages — guardianmesh stays operational. This makes the platform a natural fit for government emergency management procurement. Federal, provincial, and municipal agencies contract guardianmesh Inc. to deploy and maintain emergency communication infrastructure within their jurisdictions.

Level	Example Agencies	Contract Type	Typical Value
Municipal	BC municipal emergency mgmt	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

Note on SDK & Open-Source Strategy. The guardian-mesh-sdk is dual-licensed under AGPL-3.0 and a commercial license. The SDK will be published publicly after intellectual property protections are in place (patent filings from the seed round Legal/IP budget). Once published, the source code will be fully auditable — building trust with security-conscious government and enterprise buyers. SDK adoption and enterprise licensing are pursued as network-growth and IP-validation mechanisms, not as direct revenue streams at this stage. Non-dilutive grants (SR&ED, IRAP, PacifiCan RDII) supplement cash flow and are tracked separately from operating revenue.

The Guardian Credit Economy. guardianmesh operates an internal credit economy to incentivize relay node operators (Guardians). Revenue from all sources — government contracts, corporate sponsorships, licensing — is injected into monthly accounting periods. The company determines the credit price and the total monthly payout pool based on revenues available. Guardians are paid via a 50/50 equal-plus-proportional settlement: half split equally among all active Guardians, half proportional to relay credits earned. Credits are weighted by message priority (Emergency=100, High=25, Normal=5, Low=2, Bulk=1). Guardians may request payout via cryptocurrency or bank transfer ($5 minimum). This creates a self-sustaining loop: more revenue funds more guardian payouts, attracting more node operators, increasing network density and reliability — making the platform more valuable to the next customer.

10 Pricing Strategy

Modeled near-term revenue is government contracts only. Enterprise licensing, corporate sponsorships, and SDK commercialization are future or optional upside — not included in current financial projections. The SDK is dual-licensed (AGPL-3.0 + commercial) and will be published after IP protections are filed — not a direct revenue stream at this stage.

Government contracts are structured as multi-year agreements with an initial deployment fee plus annual support and maintenance, following Treasury Board guidelines for Canadian federal procurement.

Government Contract Framework

Component	Structure	Typical Range
Initial Deployment	Fixed fee	$50K–$250K
Annual Support & Maintenance	18–22% of deployment fee	$9K–$55K / yr

Government contracts are priced for multi-year engagement with predictable budget allocation. The Victoria SAR field trial provides real-world deployment proof and operational validation — directly supporting government contract sales. Non-dilutive grants (SR&ED;, IRAP, PacifiCan RDII) supplement operating cash flow and are applied for independently of contract revenue.

11 Go-to-Market Strategy

guardianmesh is pre-revenue by design at this stage; the immediate milestone is a funded field trial, not consumer adoption. The go-to-market approach is two-phase: validate the platform through a real SAR field trial, then win government emergency management contracts through direct procurement engagement, grant programs, and agency partnerships.

Phase 1 — Field Trial & Government Validation (Q2–Q3 2026)

- Victoria SAR field trial — funded by seed round ($75K dedicated budget), deploying Ratchet reference app with real search-and-rescue operators
- Operational validation report documenting real-world performance: BLE mesh range, message delivery reliability, evidence capture workflow, offline resilience
- PSPC Standing Offer registration initiated for federal procurement eligibility
- Municipal emergency management pilot pipeline opened (BC municipalities)
- SDK v1.0 published to npm for third-party developer adoption and network growth

Phase 2 — Government Sales & Procurement (2027)

- Government procurement: Register as Standing Offer holder with PSPC. Pursue Emergency Management BC pilot contract for wildfire season communications. Target DND (IDEaS), Public Safety Canada, and provincial emergency management agencies
- Direct outbound sales to enterprise security and IT teams at mining/forestry operations, telecom resilience, maritime operators, and critical infrastructure
- NGO pipeline: UNHCR, MSF (Doctors Without Borders), Red Cross — organizations that operate in connectivity-challenged environments
- Conference presence: USENIX Security, IEEE S&P;, DEF CON, Black Hat, RightsCon
- Federal procurement registration (PSPC supplier list for Canada, SAM.gov for US market)

Key Acquisition Channels

Channel	Audience	Primary Goal
Government Procurement	Defence, public safety agencies	Contract revenue, long-term relationships
Field Trials	SAR/Emergency agencies	Operational validation, deployment proof, procurement evidence
NGO Partnerships	Humanitarian orgs	Field validation, press coverage, grant eligibility
GitHub	Developers / Security researchers	Technical trust signals, open-source credibility
Conference Presence	PSPC, emergency mgmt agencies	Procurement pipeline, sector visibility

12 Financial Projections

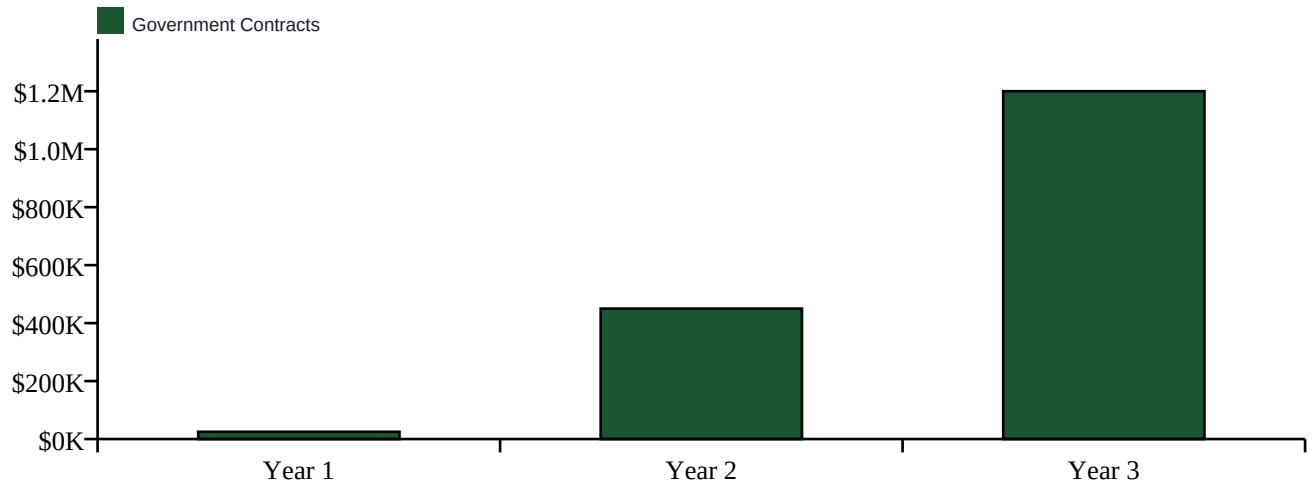
Three-year projections reflect a conservative ramp from first government pilot to multi-contract scale. All revenue is from government contracts. Year 1 focuses on securing the first municipal pilot; Year 2 on provincial expansion; Year 3 on federal contracts and full provincial scale. Non-dilutive grants (SR&ED;, IRAP, PacifiCan) supplement cash flow and are not included in these figures.

Revenue Projections

Revenue Stream	Year 1	Year 2	Year 3
Government Contracts (Base)	$25,000	$450,000	$1,200,000
Conservative Case	$25,000	$150,000–$250,000	$800,000–$1,000,000

Note on Year 2 projection: The jump from $25K (Y1) to $450K (Y2) is an 18× increase that requires multiple provincial contracts to activate within the same 12–18 month procurement cycle this document acknowledges. For Y2 revenue to be achieved, Standing Offer registration with PSPC must begin in Q1 Y1 and at least two provincial contracts must reach award by Q1–Q2 Y2. This is an optimistic but achievable scenario — not a guaranteed outcome. Investors should model a conservative case where Y2 government revenue is $150K–$250K, with $450K reached in Year 3.

Revenue by Stream — 3-Year Overview



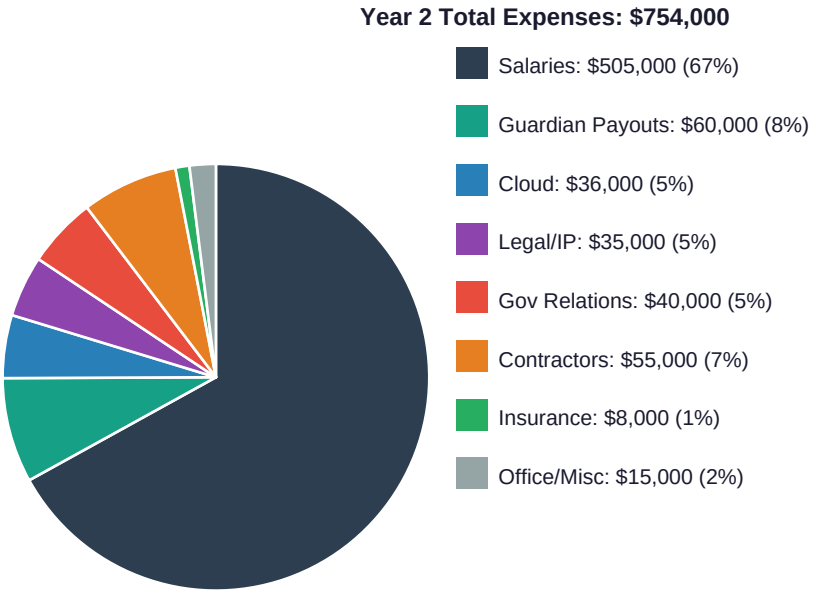
Expense Projections

Expense Category	Year 1	Year 2	Year 3
Salaries & Benefits	$435,000	$505,000	$680,000
Guardian Payouts (80% pool)	$8,000	$60,000	$180,000
Cloud Infrastructure	$24,000	$36,000	$72,000
Legal & IP	$40,000	$35,000	$35,000
Gov Relations & Conferences	$20,000	$40,000	$80,000
Contractors	$50,000	$55,000	$60,000
Insurance	$5,000	$8,000	$15,000
Office & Miscellaneous	$38,000	$15,000	$30,000
TOTAL EXPENSES	$620,000	$754,000	$1,152,000

Profit & Loss Summary

	Year 1	Year 2	Year 3
Total Revenue	$25,000	$450,000	$1,200,000
Total Expenses	$620,000	$754,000	$1,152,000
Net Income	**-$595,000**	**-$304,000**	**$48,000**
Net Margin	**-2380.0%**	**-67.6%**	**4.0%**

Year 2 Expense Breakdown



Year 1 net of -$595,000 reflects the ramp period as the first government pilot contract is secured and the guardian network is seeded. Year 2 net is -$304,000 (-67.6% margin) as provincial contracts begin coming online — the company is approaching breakeven as the government contract pipeline builds. Year 3 reaches 4.0% net margin with federal and provincial contracts at scale.

Government Procurement Timeline: 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 mechanism. Year 2 provincial contracts assume Standing Offer registration with PSPC initiated in Q1 Y1. **Net margin note:** Y3 margins of 4.0% assume government contract compliance overhead is managed within the 5-person core team scaling to 7+ as revenue grows. Contracts with significant reporting or third-party audit requirements may reduce margins by 3–7 percentage points.

13 Unit Economics

Unit economics are based on government contract values. All figures are modeled assumptions — not yet validated by paying customers. These will be updated following first paid contract.

Government Contract Economics

Metric	Value	Notes
Average Contract Value (ACV)	$150,000 / yr	Weighted average: municipal $75K, provincial $150K, federal $500K
Average Contract Duration	3 years	Multi-year agreements standard in emergency management procurement
Lifetime Contract Value (LCV)	$450,000	= $150K/yr × 3 years (excludes renewals)
Customer Acquisition Cost (CAC)	$30,000	Business development time, conferences, proposal writing, legal
LCV : CAC Ratio	15 : 1	Government contracts are large and sticky once deployed
Payback Period	~2–4 months	CAC recovered within first partial-year contract payment

Note: All unit economics are modeled assumptions based on typical government emergency management contract sizes. These will be validated against actual data following first paid contract.

Guardian Network Cost Economics

Guardians are the operational backbone of the mesh network. Unlike traditional infrastructure where the company owns servers, guardianmesh distributes infrastructure costs across a community of node operators. Each guardian runs a relay node on their own hardware (Raspberry Pi, home server, cloud VPS). The company pays them from the guardian pool — 80% of corporate-injected revenue flows to guardians, while 20% is retained for platform operations.

Metric	Value	Notes
Active Guardians (Y2 target)	200	Community-hosted relay nodes
Avg Guardian Payout	~$25 / mo	From 80% pool (50% equal + 50% proportional)

Total Annual Guardian Cost	$60,000	Network operating cost — COGS for infrastructure
Messages Relayed / Guardian / Day	~500	Average across all priority levels
Cost per 1,000 Relays	~$0.28	Guardian payout per relay unit
Network Coverage per $1 Spent	~3,500 relays	Highly efficient distributed infrastructure

Breakeven Analysis

Year 1 total projected expenses are $620,000. The seed round provides 24 months of runway; government contracts supplement that runway as they land. Breakeven depends on government contracts only — the sole revenue stream.

Scenario	Revenue Source	Annual Revenue	Covers Y1 Expenses?
Partial-year municipal pilot (Y1)	Government	$25,000	Partial (4%) — seed covers gap
Full municipal contract	Government	$75,000 / yr	Partial (12%)
1 provincial contract	Government	$150,000 / yr	Yes — 24%
2 provincial contracts	Government	$300,000 / yr	Yes — covers Y2 operations

The breakeven threshold requires a single provincial emergency management contract (~$150K/yr). Given that BC alone spends over $500M annually on wildfire response and emergency management, capturing even a fraction of one percent of that budget covers guardianmesh's entire Year 1 operating expenses.

PART IV

Funding Strategy

This section details guardianmesh Inc.'s capital formation strategy — the investment already made, the non-dilutive grant programs available, the angel and venture capital landscape, and the precise allocation of the seed round being sought. The company enters fundraising with a fully built product, proven technology, and a defensible IP portfolio.

14 Investment to Date

Founder Sweat Equity

Bruce deGrosbois has invested 2 years of intensive, full-time development at 10 hours per day, 6 days per week. At a market rate of $100/hour for senior full-stack/cryptographic engineering, this represents:

Component	Value
Years of development	2 years
Weeks per year	52 weeks
Days per week	6 days
Hours per day	10 hours
Market rate (senior full-stack / cryptographic)	$100/hour
Total Sweat Equity	$624,000

2 years × 52 weeks × 6 days × 10 hours × $100/hour = $624,000

Cash Investment

Source	Amount
Founder (Bruce deGrosbois)	$15,000
Wendy Wilkins	$2,000
Michelle Corbett	$2,500
Total Cash	$19,500

What the Investment Produced

Deliverable	Metric
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, gateway + routing + obfuscation
Mobile app	iOS + Android via Expo

Enterprise backend	Operations stack: accounting, HR, governance, investor services
Security architecture	6-layer defense-in-depth, formal threat model, third-party audit planned
Whitepaper	Academic-quality, targeting top-tier venues
Federal incorporation	CBCA Corp #1775511-2

$643,500 in founder commitment and direct cash — proof of technical execution prior to external capital ($624,000 sweat equity + $19,500 cash). Company valuation is forward-looking and based on revenue potential, not cost-basis.

15 Government Grants & Contracts Strategy

guardianmesh Inc.'s government strategy operates on two parallel tracks: (1) **government contracts** — the company's primary revenue stream, where agencies procure emergency communication infrastructure as an ongoing operational service; and (2) **non-dilutive grants** — R&D funding programs that subsidize technology development without generating recurring revenue. The distinction is critical: contracts fund operations and pay guardians; grants fund research and extend runway.

Government Contract Pipeline

Agency Type	Use Case	Contract Structure	Target Value
Municipal Emergency Mgmt	Wildfire/flood comms backup	Annual service contract	$50K–$100K / yr
Provincial Emergency Mgmt	Province-wide emergency mesh	Multi-year deployment	$100K–$250K / yr
Indigenous Services Canada	Remote community connectivity	Federal program contract	$150K–$500K / yr
DND / Canadian Forces	DDIL tactical communications	IDEaS procurement → contract	$250K–$1M+ / yr
Public Safety Canada	Critical infrastructure resilience	CSSP → operational contract	$200K–$500K / yr

Canada offers one of the most generous non-dilutive funding ecosystems in the world for deep-tech startups. guardianmesh Inc. is uniquely positioned to access multiple federal and provincial programs given its focus on cryptographic infrastructure, privacy technology, and national security applications. Non-dilutive funding extends runway, de-risks development milestones, and preserves equity for strategic investors.

Federal Programs

Program	Amount	Type	Timeline
SR&ED; + BC Credit	~$36K–$250K+/yr	Tax credit (45% combined)	Annual filing
NRC IRAP	Up to $500K	Non-repayable grant	Rolling intake
PacifiCan RDII	Varies ($67.5M fund)	Grant	Apr 15, 2026 deadline
CSIN / NCC	$25K–$2.5M	Grant	2027 call expected

IDEaS (DND)	Up to $1.2M	Contract	Call-based
CSSP (Public Safety)	Up to $2M	Grant	Call-based
Mitacs Accelerate	$15K/intern	Grant	Ongoing
CanExport Innovation	Up to $37.5K	Grant	Rolling
NSERC Alliance	$20K–$1M/yr	Grant	University partner needed

SR&ED Eligibility: guardianmesh Inc.'s R&D activities — including novel cryptographic protocol implementation, DTN algorithm development, and mesh networking optimization — qualify as systematic investigation under SR&ED. At 35% federal + 10% BC credit on eligible expenditures, early-year claims could yield **$36K–$50K+ in refundable credits**.

BC Provincial Programs

Program	Amount	Type
Innovate BC	Up to $500K	Early-stage demonstration
New Ventures BC	$250K+ prizes	Competition
BC VCTC	30% investor tax credit	EBC registration needed
AccelerateIP	Free IP strategy + patent	Ends Mar 31, 2026
CDL-Vancouver	Network / mentors	Accelerator
SFU VentureLabs	Deeptech accelerator	No affiliation required

Key Program Deep Dives

NRC IRAP — Industrial Research Assistance Program

IRAP is Canada's premier innovation assistance program, offering up to $500K in non-repayable contributions for SMEs conducting R&D.; An Industrial Technology Advisor (ITA) is assigned to each applicant. guardianmesh Inc. qualifies based on: (1) Canadian incorporation (CBCA), (2) fewer than 500 employees, (3) proprietary technology under active development. The mesh cryptography stack, DTN routing, and AI automation platform each constitute eligible R&D; activities. IRAP funds can cover salaries for technical staff working on approved projects.

PacifiCan RDII — Regional Defence Investment Initiative

Pacific Economic Development Canada's $67.5M Regional Defence Investment Initiative targets BC-based businesses developing technologies with defence and dual-use applications, including artificial intelligence, quantum technologies, and cyber security. The April 15, 2026 deadline represents an immediate priority. guardianmesh Inc.'s censorship-resistant mesh network, cryptographic infrastructure, and emergency communication capabilities directly align with RDII's mandate to build BC's defence industrial capacity and supply chain readiness.

IDEaS (DND) and CSSP (Public Safety Canada)

The Department of National Defence's Innovation for Defence Excellence and Security (IDEaS) program and the Canadian Safety and Security Program (CSSP), managed by DND/DRDC, both fund technologies with national security applications. guardianmesh's censorship-resistant mesh network, post-quantum cryptography roadmap, and emergency communication

capabilities directly address federal priorities around critical infrastructure protection and resilient communications. IDEaS contracts run up to $1.2M; CSSP grants up to $2M.

Grant Pursuit Roadmap

Phase	Timeline	Programs	Target Funding
Near-Term	Q2 2026	SR&ED; filing, IRAP application, PacifiCan RDII submission	$36K–$536K+
Mid-Term	Q3–Q4 2026	CSIN preparation, Mitacs internships, Innovate BC, New Ventures BC	$100K–$600K
Long-Term	2027	IDEaS call, CSSP call, NSERC Alliance (university partner)	$500K–$3.2M

Non-dilutive funding extends runway and de-risks development, but the company's long-term revenue model depends on converting government relationships from one-time grants into recurring operational contracts. Every grant application is also a relationship-building exercise with the contracting agency. The company's deep-tech profile, Canadian domicile, and national security relevance create an unusually strong pipeline that most seed-stage startups cannot access.

16 Angel & VC Strategy

guardianmesh Inc. will pursue a staged capital formation strategy, beginning with angel investors who can provide patient capital and operational guidance, followed by institutional venture capital as revenue traction and product milestones are demonstrated. British Columbia's investor tax credit program significantly enhances the economics for early-stage investors.

BC Angel Networks

Network	Focus	Notes
VANTEC Angel Network	Technology, deep tech, B2B SaaS	Vancouver's largest angel group; monthly pitch events; strong tech sector network
Keiretsu Forum Vancouver	Broad technology, healthcare, consumer	Global network chapter; rigorous due diligence process; post-investment support
Angel Forum Society	Early-stage BC companies	BC-focused; connects founders with accredited investors; pitch competition format

BC Venture Capital Tax Credit Advantage: The BC Venture Capital Tax Credit (VCTC) provides angels with a **30% provincial tax credit** on investments in eligible BC companies. guardianmesh Inc. intends to register as an Eligible Business Corporation (EBC) to offer this benefit to investors — effectively reducing the net cost of a $100K investment to $70K while retaining full upside participation.

Target Venture Capital Firms

The following Canadian venture firms have investment theses aligned with cybersecurity, privacy infrastructure, and developer tooling — the three primary value propositions of guardianmesh Inc.:

Firm	Focus	Stage	Location

Vanedge Capital	Deep tech, cybersecurity, enterprise	Seed–Series A	Vancouver, BC
Version One Ventures	B2B SaaS, developer tools, infrastructure	Seed–Series A	Vancouver, BC
Panache Ventures	Emerging tech, pre-seed/seed	Pre-seed–Seed	Pan-Canadian
Inovia Capital	Tech infrastructure, security, scale-ups	Series A–B	Montreal/Vancouver

Alternative & Non-Dilutive Debt Financing

Instrument	Provider	Amount / Terms	Suitability
Revenue-Based Financing	TIMIA Capital	$500K–$10M; repaid as % of revenue	Post-revenue; preserves full equity
Equity Crowdfunding	FrontFundr	Up to $1.5M under offering memorandum	Community investors; brand building

The equity crowdfunding route via FrontFundr is particularly attractive as a brand-building exercise: engaging the developer and privacy communities as micro-investors creates a base of vocal advocates while raising capital under the offering memorandum exemption without requiring a full prospectus.

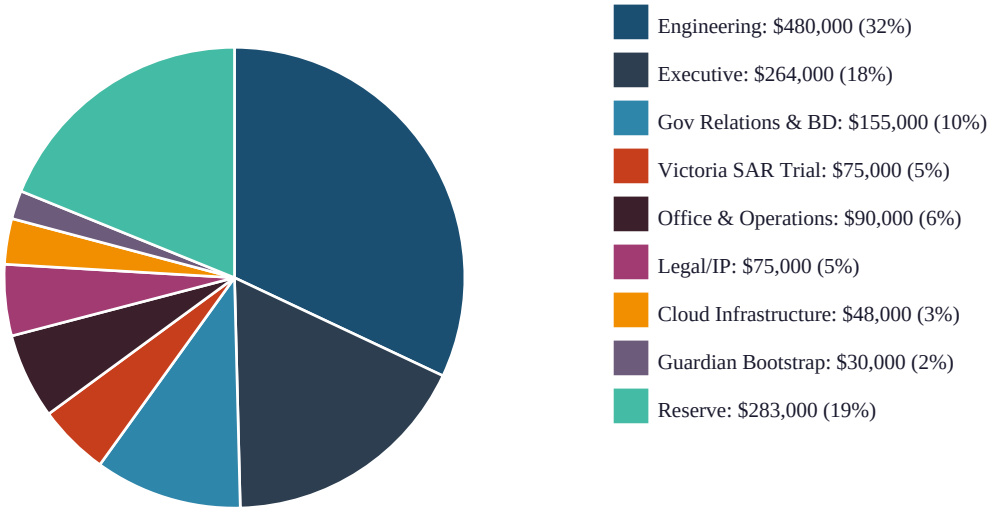
17 Use of Funds

Upon closing a $1,500,000 seed round, guardianmesh Inc. will deploy capital across eight categories designed to achieve product-market fit, complete the Victoria SAR field trial, and establish IP defensibility within 24 months. The allocation prioritizes engineering execution and government contract validation while maintaining a prudent operational reserve.

$1.5M Seed Round Allocation

Category	Amount	%	Purpose
Engineering	$480,000	32%	Senior engineer + junior developer (24 months)
Executive	$264,000	18%	CEO + Founder/Technical Evangelist (partial — revenue supplements)
Gov Relations & BD	$155,000	10%	Head of Gov Relations & BD + conference/travel budget
Victoria SAR Trial	$75,000	5%	Equipment, travel Van→Vic, training, field ops
Office & Operations	$90,000	6%	Vancouver office, insurance, admin, tools
Legal/IP	$75,000	5%	2–3 patent filings, trademark, counsel
Cloud Infrastructure	$48,000	3%	AWS/GCP hosting for 24 months
Guardian Bootstrap	$30,000	2%	Early operator payouts to seed relay network
Reserve	$283,000	19%	3-month runway buffer + contingency
TOTAL	**$1,500,000**	**100%**	

Allocation by Category



24-Month Runway Plan

The $1.5M seed round, combined with projected grant income (SR&ED;, IRAP) and early revenue from government contracts, provides a 24-month operational runway. The reserve allocation ($283,000) ensures the company can weather delays in grant disbursements or procurement timelines. The Victoria SAR field trial ($75,000) is a dedicated line item — this pilot is the revenue unlock that validates the platform for provincial and federal procurement. Key milestones: (1) Victoria SAR field trial completed, (2) first government pilot contract signed, (3) SDK v1.0 public release on npm, (4) 200+ active guardian node operators, (5) Series A readiness with demonstrated revenue growth. Engineering hiring is sequenced to begin in Month 1 with a senior backend engineer, followed by a junior developer in Q2.

18-Month Milestone Targets

Timeline	Milestone	Budget Driver
Month 1–2	Engineering hires onboarded; IP counsel retained	Engineering + Legal/IP
Month 3–6	SDK v1.0 published; 50 company-operated seed nodes + SAR trial operators	Cloud Infra + Field Trial
Month 6–9	First government pilot contract; SR&ED; + IRAP disbursed	Gov Relations + Engineering
Month 9–12	200 guardian nodes (seed + trial + SDK adopters); Series A materials	Operations + Reserve
Month 12–18	Series A raise; patent filings complete	Legal/IP + Reserve

PART V

Team & Execution

Behind every line of code and every architectural decision is a founder with 25 years of software development experience and a clear vision: communication that works when nothing else does. This section covers the team, the hiring plan, the product roadmap, and the risks that have been identified and mitigated along the way.

18 Team & Hiring

Founder Profile

Bruce deGrosbois — Founder & Technical Evangelist. 25 years of software development experience. Built first successful platform in 2002. Sole architect and developer of the entire guardianmesh platform: 182,000+ lines of production code, 9,000+ automated tests (525 files), 34 novel IP innovations. Implemented Signal Protocol (X3DH + Double Ratchet), MLS RFC 9420, and Noise XX handshake from specification. Transitioning from sole developer to Technical Evangelist role: representing guardianmesh at conferences and tech events, coordinating field trials with SAR and emergency services, developer outreach, and partnership development.

Planned Leadership Team (5 people, funded by seed round):

- **CEO** — Business operations, investor relations, government procurement
- **Head of Gov Relations & BD** — Government procurement pipeline, field trial coordination, grant applications, emergency services partnerships
- **Senior Engineer** — Backend/infrastructure: Python, TypeScript, API scaling
- **Junior Engineer** — Mobile + frontend: React Native, BLE, testing
- **Bruce deGrosbois (Founder & Technical Evangelist)** — Conference representation, SAR partnerships, developer advocacy, field trial coordination

Team Build-Out (Seed-Funded)

Timeline	Role	Focus
Month 1	CEO	Business operations, investor relations, government procurement pipeline
Month 1	Head of Gov Relations & BD	Government procurement, field trial coordination, grant applications, partnerships
Month 1	Founder & Technical Evangelist	Conference representation, SAR partnerships, developer advocacy, field trials
Month 2	Senior Engineer	Python/TypeScript backend, API scaling, infrastructure hardening
Month 3–4	Junior Engineer	React Native mobile, BLE integration, testing, frontend
Q1 2027	Security Engineer	Third-party audit, penetration testing, compliance certifications
Q2 2027	Sales Engineer	Enterprise deals, government procurement, technical sales support
Q3 2027	Product Manager	Roadmap prioritization, user research, enterprise requirements
Q4 2027	Infrastructure Engineer	Scaling, monitoring, SRE practices, Guardian node reliability

Advisory Board Targets

Cybersecurity Expert: Deep cryptographic engineering expertise, ideally with experience in offensive security or standards bodies (IETF, NIST).

Telecom / Mesh Veteran: Operational experience deploying mesh networking infrastructure at scale, including rural, maritime, or emergency deployments.

Canadian VC / Angel Investor: Network and pattern recognition for Canadian deep-tech fundraising, SR&ED; optimization, and IRAP/NRC grant strategy.

Government Procurement Specialist: Experience with DND IDEaS, CSIN, NCC, and navigating Public Services and Procurement Canada (PSPC) processes for technology acquisitions.

Mitacs Internships: guardianmesh Inc. plans to leverage Mitacs Accelerate and Globalink programs to access subsidized research talent from Canadian universities. This provides additional development capacity via a $15K/intern grant, supports academic paper submission goals, and creates a pipeline for full-time hiring.

19 Roadmap & Milestones

The 36-month roadmap is structured around five key value-creation events: SDK publication, first government contract, developer community growth, government grant funding, and profitability at ~$2M ARR. Each milestone has a measurable KPI to track progress objectively.

Quarter	Milestone	KPI
Q2 2026	Victoria SAR field trial begins	Reference deployment with real SAR operators in field conditions
Q2 2026	SDK v1.0 published to npm	Third-party developer adoption begins
Q2 2026	SR&ED; filing, IRAP application	Grant submissions complete, confirmation numbers received
Q3 2026	Victoria SAR trial complete; validation report delivered	Operational evidence for government procurement
Q3 2026	PSPC Standing Offer registration initiated	RFQ filed — government procurement vehicle active
Q4 2026	First government pilot contract signed	Emergency comm deployment for BC municipality — first paid contract
Q1 2027	CSIN/NCC application submitted	Grant pipeline — cybersecurity grant applications filed
Q1 2027	Academic paper submitted	Conference acceptance — USENIX, IEEE S&P;, or ACM CCS
Q2 2027	500+ SDK AGPL installs	Network density metric — open-source adoption validates deployment readiness
Q3 2027	DND IDEaS pursuit	Defence contract pipeline — IDEaS Phase 1 application filed
Q4 2027	$1.2M government contract run-rate	Profitability — positive operating cash flow on government contracts alone

Network Effect Strategy: The SDK-first go-to-market strategy is designed to bootstrap network effects through government deployments and SDK adoption. Each third-party developer who integrates the guardianmesh SDK adds their users as potential relay nodes. This means that SDK adoption and relay network growth are directly correlated — as adoption grows, relay density increases, which improves coverage for all participants (field trial operators, SDK integrators), which makes the platform more valuable to the next SDK customer. This self-reinforcing flywheel is the core strategic asset: competitors cannot replicate it by simply copying the codebase — they would need to replicate the entire relay network as well.

20 Risk Analysis

Every technology venture carries inherent risks. The risks below have been identified, categorized, and mitigated to the greatest extent possible given the current stage of the company. Investors should review this analysis alongside the financial projections and sensitivity analysis in Appendix D.

Risk	Category	Probability	Impact	Mitigation
Key person dependency	Operational	High	Critical	5-person team from close (CEO, Gov Relations & BD, 2 engineers, Founder), comprehensive documentation, 9,000+ tests as living executable spec, clean modular architecture
Slow SDK adoption	Market	Medium	High	Free AGPL tier, developer community, content marketing, Mitacs interns
Competitor with more funding	Market	Medium	Medium	Technical moat (34 IPs), first-mover advantage, network effects defensibility
Regulatory changes (encryption)	Regulatory	Low	High	Canadian CBCA jurisdiction, legal counsel on retainer, AGPL open-source auditability
Security vulnerability	Technical	Medium	Critical	Audited @noble/* crypto libraries, 9,000+ tests, responsible disclosure policy
Grant applications rejected	Financial	Medium	Medium	Multiple simultaneous applications, diversified funding (IRAP, SR&ED;, CSIN, IDEaS)
Government procurement delay	Financial	High	High	12–18 month procurement cycles are modeled; conservative case ($150K–$250K Y2) buffers for slippage. Multiple parallel procurement channels (municipal, provincial, federal). Non-dilutive grants extend runway independently of contract timing.
Enterprise adoption slower than expected	Market	Medium	Low	Government contracts are primary revenue; enterprise/SDK adoption is parallel upside, not a dependency
App store rejection	Technical	Low	Medium	P2P APK distribution via mesh (IP-028), progressive web app fallback available
Network bootstrap (chicken-and-egg)	Technical	Medium	High	Government pilot contracts seed the network, SDK adoption supplements relay density, company-operated seed nodes bootstrap coverage
Team hiring difficulty	Operational	Medium	Medium	Remote-first culture, competitive equity compensation, Mitacs internship pipeline

Key Person Risk — Substantially Mitigated: The seed round funds a 5-person team from Month 1, eliminating single-person dependency. The founder transitions from sole developer to Technical Evangelist, with a dedicated CEO handling operations and two engineers maintaining the codebase. Additional mitigations: (1) **Comprehensive documentation** — every protocol, architecture decision, and operational procedure is documented. (2) **9,000+ automated tests as living documentation** — executable specification that any competent engineer can use to understand the system. (3) **Clean modular architecture** — clearly bounded modules with explicit interfaces. (4) **5-person team from close** — CEO, Head of Gov Relations & BD, Senior Engineer, Junior Engineer, and Founder all onboard within the first 90 days of funding. No single point of failure.

A Appendix A: Codebase Metrics

The guardianmesh platform is an unusually complete pre-revenue technology platform: 182,000+ lines of production code, 9,000+ automated tests across 100 test suites, and 34 distinct IP innovations — all built by a single founder over approximately two years. Most seed-stage companies present an MVP; guardianmesh presents a production-ready, internally validated system with third-party security audit planned post-funding.

Lines of Code Breakdown

Component	Approx LoC	Language	Tests
guardian-mesh-sdk	~28,000	TypeScript	262 tests, 25 suites
guardianmesh (servers)	~35,000	TypeScript	Included in SDK tests
guardianmesh-py (backend)	~45,000	Python	113 test files
ratchet (app + packages)	~74,000	TypeScript/React Native	1,683 tests, 75 suites
Total	**~182,000+**		**9,000+ tests, 525 files**

Test Coverage Summary

Project	Statements	Branches	Functions	Lines	Threshold Met
guardian-mesh-sdk + guardianmesh	80.32%	65.28%	61.53%	82.75%	✓
ratchet (packages + mobile)	83.6%	79.83%	85.3%	84.16%	✓
Thresholds (ratchet)	≥82%	≥78%	≥72%	≥84%	All Met

Dependency Audit — Security-Critical Libraries

@noble/curves: Audited, zero-dependency pure-JavaScript elliptic curve library. Provides Ed25519 signing and X25519 key agreement. Used for identity and key exchange throughout the platform.

@noble/hashes: Audited, zero-dependency pure-JavaScript cryptographic hash library. Provides SHA-256, SHA-512, HKDF, HMAC. Used in KDF chains, identity hashing, and relay receipt signing.

@noble/ciphers: Audited, zero-dependency pure-JavaScript symmetric cipher library. Provides AES-256-GCM authenticated encryption. Used in all message encryption paths and secure enclave storage.

@msgpack/msgpack: MessagePack codec for efficient binary message serialization. Used in the protocol layer for compact wire encoding of all message types.

pako: zlib compression library. Used for bundle compression in the DTN layer to reduce relay bandwidth requirements.

React Native / Expo SDK 55: Cross-platform mobile framework. Used for the Ratchet mobile app (iOS + Android). Expo SDK 55 provides stable native module APIs and BLE peripheral support via @dr.pogodin/react-native-static-server.

B Appendix B: IP Innovation Catalog

guardianmesh Inc. has identified 34 distinct intellectual property innovations across the platform. These innovations span algorithmic, economic, security, architectural, infrastructure, documentation, and process categories. Each is classified by IP type and business priority for patent, trade secret, and copyright protection strategy.

ID	Name	Category	IP Type	Priority
IP-001	Hop-Based TTL for DTN	Algorithm	Patentable	Critical
IP-002	Tiered Bloom Filters with Emergency Bypass	Algorithm	Patentable	Critical
IP-003	Two-Stage Dead-Man Alert	Algorithm	Patentable	Critical
IP-004	Network Witness Protocol	Algorithm	Patentable	Critical
IP-005	Adaptive Battery-Aware Cover Traffic	Algorithm	Patentable	High
IP-006	Multi-Method Cascading Discovery	Algorithm	Patentable	High
IP-007	Earned-Only Credit System	Economic	Trade Secret	High
IP-008	50/50 Equal + Proportional Settlement	Economic	Patentable	Critical
IP-009	Credit Account Persistence via HKDF	Economic	Patentable	High
IP-010	Relay Diversity Weight	Economic	Trade Secret	Medium
IP-011	Priority-Weighted Credits with Federation Multiplier	Economic	Trade Secret	Medium
IP-012	Duress PIN with Decoy Account	Security	Patentable	High
IP-013	Ed25519-Only Authentication	Security	Trade Secret	Medium
IP-014	5-Level Web-of-Trust	Security	Patentable	High
IP-015	Noise XX Handshake with DPI-Resistant Key Exchange	Security	Patentable	High
IP-016	Warrant Canary System	Security	Copyright	Medium
IP-017	APK Transparency Log	Security	Patentable	Medium
IP-018	Guardian Mesh Federation Protocol	Architecture	Trade Secret	High
IP-019	Online Logistic Regression Peer Scorer	Architecture	Patentable	High
IP-020	Composite Guardian Health Score	Architecture	Trade Secret	Medium
IP-021	Context-Aware Transport Selection	Architecture	Patentable	Medium
IP-022	Onion Routing for Mobile DTN	Architecture	Copyright	Medium
IP-023	Reed-Solomon Erasure Coding (WASM)	Architecture	Copyright	Medium
IP-024	Secure Deletion via Partition Key Rotation	Architecture	Trade Secret	Medium
IP-025	Sneakernet Transport (QR + File)	Infrastructure	Patentable	Medium
IP-026	Satellite/Radio Gateway	Infrastructure	Copyright	Medium
IP-027	Diaspora Bridge	Infrastructure	Patentable	Medium
IP-028	P2P APK Distribution via Mesh	Infrastructure	Patentable	Medium
IP-029	BLE Peripheral Mode with GATT Server	Infrastructure	Trade Secret	Medium
IP-030	Traffic Obfuscation Layer	Infrastructure	Copyright	Medium
IP-031	Academic-Quality Whitepaper	Documentation	Copyright	High
IP-032	Comprehensive Threat Model	Documentation	Trade Secret	Medium
IP-033	Reproducible Builds System	Process	Copyright	Medium
IP-034	7-Day Soak Test Automation	Process	Trade Secret	Low

Summary by Category and IP Type

Category	Count	IP Type	Count	Priority	Count
Architecture	7	Patentable	17	Critical	5
Algorithm	6	Trade Secret	10	High	10
Security	6	Copyright	7	Medium	18
Infrastructure	6			Low	1
Economic	5				
Documentation	2				
Process	2				

C Appendix C: Grant Program Details

guardianmesh Inc. is eligible for multiple Canadian government grant and incentive programs. The following details the top five programs by priority, including eligibility requirements, calculation methods, and filing requirements.

1. SR&ED; — Scientific Research and Experimental Development

Canada Revenue Agency (CRA) — Up to 35% refundable tax credit (CCPC) on eligible R&D; expenditures

Eligible Activities: Experimental development of new software protocols, cryptographic algorithm implementation (X3DH, Double Ratchet, MLS RFC 9420, Noise XX), novel transport layer integration, DTN routing algorithms, and incentive mechanism design. All 34 IP innovations qualify as experimental development under CRA guidelines.

Calculation Method: 35% refundable federal credit on first $3M of eligible expenditures for Canadian-controlled private corporations (CCPC), plus an additional 10% BC Scientific Research and Experimental Development Tax Credit (BC SRED) — 45% combined. Eligible costs include salary (founder sweat equity can be partially claimed), contractor costs, and overhead. Estimated Y1 claim: $30,000–$50,000 based on documented development expenditures.

Filing Requirements: Form T661 (SR&ED; Expenditures Claim) filed with T2 corporate tax return. Technical narrative required documenting the systematic investigation, technological advancement, and uncertainty. CRA recommends pre-filing consultation with SR&ED; officer. Deadline: 18 months after fiscal year-end.

2. NRC IRAP — Industrial Research Assistance Program

National Research Council Canada — $50,000–$500,000+ in non-repayable contributions for R&D; projects

Eligibility: Canadian-incorporated SME (under 500 employees, which guardianmesh Inc. meets as a pre-revenue startup), incorporated in Canada (CBCA — confirmed), conducting R&D; with commercial potential. The SDK publication and commercialization roadmap directly aligns with IRAP commercial-potential criteria.

Process: Initial contact with an IRAP Industrial Technology Advisor (ITA) assigned to the region (Victoria, BC). ITA assesses technical merit and commercial potential. If supported, a formal work plan is developed with the ITA and a contribution agreement executed. Funding is disbursed as milestone payments tied to approved R&D; activities (hiring, prototyping, testing). Typical approval timeline: 60–90 days.

guardianmesh Alignment: SDK commercialization, BLE transport optimization, enterprise API development, and security audit all qualify as IRAP-eligible R&D; activities. Target: $150,000 contribution for Q2–Q4 2026 engineering activities.

3. PacifiCan RDII — Regional Development Innovation Initiative

Pacific Economic Development Canada (PacifiCan) — Up to $1M+ for BC-based technology innovation projects

Eligibility: BC-based incorporated business (guardianmesh Inc. registered in Victoria, BC), focused on technology innovation with economic development impact for the Pacific Region. Cybersecurity and communications infrastructure are priority sectors.

Focus: The RDII is a $67.5M fund supporting innovation projects that create jobs and economic value in BC. guardianmesh SDK commercialization creates high-value tech jobs in Victoria and positions BC as a hub for privacy-preserving communication technology.

Deadline: April 15, 2026 for current intake. Application requires project description, budget, team qualifications, and commercialization plan. guardianmesh will target $200,000–$500,000 for engineering and market development activities.

4. CSIN — Canadian Safety and Security Program / National Cybersecurity Consortium

Public Safety Canada / NCC — Variable — project-based cybersecurity research funding

Cybersecurity Focus: CSIN and the National Cybersecurity Consortium (NCC) fund projects that advance Canadian cybersecurity capabilities, including privacy-preserving communications, critical infrastructure protection, and threat-resistant networking.

guardianmesh Alignment: The guardianmesh platform directly addresses Canadian cybersecurity priorities: resilient emergency communications, protection of journalist and activist sources, and post-quantum-ready cryptographic architecture. The 34 IP innovations and formal threat model demonstrate the depth of cybersecurity research.

Application Timeline: CSIN and NCC funding is call-based — applications are accepted during specific intake windows rather than on a rolling basis. guardianmesh will monitor for open calls and submit Q1 2027 after completing SR&ED; and IRAP processes, and after academic paper submission demonstrates research credibility. Target: $100,000–$300,000 for security research and audit activities.

5. IDEaS — Innovation for Defence Excellence and Security

Department of National Defence (DND) Canada — Up to $1.2M per project (Challenge problem pursuits)

Defence Innovation Mandate: IDEaS funds Canadian innovations that address specific defence and security challenges, including communications in denied, degraded, intermittent, and limited (DDIL) environments — which is precisely what guardianmesh is designed for.

Mesh Communications for Military: The guardianmesh SDK's multi-hop BLE mesh, LoRa transport, satellite gateway, and DTN store-and-forward routing are directly applicable to tactical military communications where cellular infrastructure is unavailable or compromised.

Application Path: IDEaS solicitations are posted as Challenge problems. guardianmesh will monitor IDEaS solicitations for DDIL communications challenges and submit a Phase 1 application in Q3 2027 after establishing proof of SDK traction and an initial enterprise customer. Target: Phase 1 ($250,000) leading to Phase 2 ($1M+).

D Appendix D: Financial Assumptions

The financial projections in Sections 12 and 13 are based on the following conservative assumptions. All figures are in Canadian dollars (CAD). A sensitivity analysis is provided at the end of this appendix.

Revenue Assumptions

Government Contracts (sole revenue stream):

Y1: 1 partial-year municipal pilot contract at $25,000 — pipeline begins at funding close; contract signed Q3–Q4 Y1 via Small Value Procurement. Y2: 2 provincial contracts at $150,000 each + expanded municipal ($100,000) + Y1 pilot deferred balance ($50,000) = $450,000. Y3: 1 federal contract ($500,000 DND/Public Safety) + 3 provincial ($150,000 each) + municipal ($150,000) = $1,200,000. Government sales cycles are 12–18 months for new vendors; Y2+ assumes Standing Offer registration with PSPC initiated in Q1 Y1.

Non-Dilutive Grants (supplemental, not in revenue figures):

SR&ED; tax credits, IRAP, and PacifiCan RDII are pursued in parallel and supplement operating cash flow but are not included in revenue projections. Estimated grant income: Y1 $50K–$100K (SR&ED; + IRAP application), Y2–Y3 ongoing as R&D; spending scales.

SDK & Enterprise (adoption — not direct revenue at this stage):

The SDK is dual-licensed (AGPL-3.0 + commercial) and will be published after IP protections are filed. Enterprise deployments contribute to network density and IP validation. Commercial SDK licensing is a future revenue opportunity. Commercial SDK licensing and enterprise network licensing are deferred revenue opportunities for a future funding round.

Expense Assumptions

Salaries:

Y1: $435,000 (CEO $120K + Gov Relations $95K + Founder $100K + Sr Engineer $110K partial year + Jr Engineer $80K partial year). Y2: $505,000 (full 5-person team: CEO, Gov Relations, Founder, Sr Eng, Jr Eng). Y3: $680,000 (5 core team + additional hires funded from revenue).

Guardian Payouts:

Y1: $8,000 (small network, ~50 guardians, funded from corporate injection). Y2: $60,000 (~200 guardians, $25/guardian/month average). Y3: $180,000 (~500 guardians, $30/guardian/month average). The company determines credit pricing and total monthly payout pool from available revenue. Guardians are paid via 50% equal + 50% proportional settlement.

Cloud Infrastructure:

Y1: $24,000 (Guardian relay servers, CI/CD, monitoring). Y2: $36,000 (scaling to support enterprise customers and growing relay network). Y3: $72,000 (multi-region deployment, enterprise SLAs, redundancy).

Legal / IP:

Y1: $40,000 (patent application filing for 2–3 critical IPs, trademark, counsel). Y2: $35,000 (additional patent filings, enterprise contract legal review). Y3: $35,000 (ongoing IP protection, licensing agreements, compliance).

Gov Relations & Conferences:

Y1: $20,000 (developer community, content, conference presence, gov events). Y2: $40,000 (conference sponsorship, enterprise marketing, government relations). Y3: $80,000 (demand generation, PR, expanded government relations).

Contractors / Field Trials:

Y1: $50,000 (Victoria SAR field trial — equipment, travel Van→Vic, training). Y2: $55,000 (expanded field trials $25K + Vancouver office $30K). Y3: $60,000 (scale-up project contractors, additional trial sites).

Sensitivity Analysis

The following tables present outcomes under three scenarios: base case (the projections used throughout this plan), a best case (+30% revenue), and a worst case (-30% revenue). Expenses are held constant in the revenue table; the second table stress-tests expense scenarios independently. All figures are in CAD thousands.

Scenario	Y1 Revenue	Y2 Revenue	Y3 Revenue
Best (+30%)	$32K	$585K	$1,560K
Base	$25K	$450K	$1,200K
Worst (-30%)	$18K	$315K	$840K

Base case Year 3 net: $48,000 (4.0%). Worst case (-30% revenue) Year 3 net: -$312,000 — a deficit of $312,000 against $1,152,000 in expenses. This would require bridging via government grants (SR&ED;, IRAP) or extending runway into Year 4. The seed round is sized for 24 months of runway; a worst-case Year 3 does not threaten solvency if grants are secured in parallel.

Expense Sensitivity — Year 3

Scenario	Y3 Expenses	Y3 Net (base rev)	Implication
Base case	$1,152,000	$48,000	Target scenario
Hiring delay (–25% salary)	$982,000	$218,000	Slower team growth; founder remains primary resource longer
Cost overrun (+20% all expenses)	$1,382,400	-$182,400	Higher compliance overhead, IP legal costs, or cloud scaling

guardianmesh Inc.

Resilient. Decentralized. Private.

guardianmesh Inc. has built the only platform that combines multi-transport offline resilience, self-sovereign identity, cryptographic relay incentives, and open-source auditability in a single production-ready SDK. With 182,000+ lines of code, 9,000+ automated tests, and 34 novel IP innovations, the technical foundation is complete. The seed round funds the team and go-to-market execution to turn this technical achievement into a category-defining company.

7	6-Layer	9,000+	34	182K+	~$644K
Transport Types	Security	Tests	IP Innovations	Lines of Code	Invested

guardianmesh Inc. • Corporation No. 1775511-2 • CBCA • Victoria, BC