

Project Name

NTN-Backhauled Helium IoT Smart Hub + Smart TOTE Risk Intelligence for AI Supply-Chain Risk Monitoring

1) Executive Summary

Logistics operators managing high-value and cold-chain shipments experience significant losses and compliance risk due to delayed detection of temperature excursions, tampering, route anomalies, and device downtime—especially at sites with limited terrestrial backhaul. This project will deliver an NTN-backhauled Helium IoT Data-Only Hotspot Smart Hub and a Helium-native risk monitoring application (“Smart TOTE Risk Intelligence”) that routes LoRaWAN telemetry through the Helium IoT Network and converts it into AI-driven risk scoring, real-time alerts, incident reporting workflows, and predictive maintenance insights.

This project benefits the Helium Network by enabling a repeatable enterprise deployment model that increases active Helium IoT gateways and endpoint activity, and produces sustained, measurable Helium IoT traffic from commercial logistics operations—validating decentralized wireless performance in demanding supply-chain environments.

- **Grant Requested:** US\$250,000
- **Project Duration:** 18 months
- **Primary Deliverables:**
 - i. Helium IoT Data-Only Hotspot Smart Hub with NTN backhaul
 - ii. Helium-native data pipeline and AI risk monitoring application (alerts, dashboards, incident reports)
 - iii. Field-validated deployment and operations readiness, plus monthly network usage and outcome reporting

Helium Foundation Criteria Alignment

This proposal is written to match the Helium Foundation “Build Helium Native Applications” criteria:

- **Viable Business Plan:** A subscription business (per monitored asset / lane / site) with optional managed deployment/operations services. Validation is planned with prospective logistics partners (e.g., Arviem and Vector), subject to 2026 alignment and pilot onboarding.

- **Capable Team:** Cross-functional delivery across gateway integration, cloud data engineering, ML, and field operations, with planned pilot validation via prospective partners once briefed and aligned.
- **Clear milestones:** A milestone-based execution plan with acceptance criteria and tranche-based funding (see milestone table).
- **Sustainable Impact:** Measurable Helium IoT usage impact (active hubs/endpoints, packets, delivery rate, sustained activity) plus quantified operational outcomes (alert quality, incident response, device uptime).

2) Problem and Opportunity

Problem

Supply-chain visibility is often fragmented across sensors, trackers, carrier systems, and manual processes. This creates three persistent operational issues:

- Late detection of excursions/tampering → higher loss severity and slower mitigation
- Excess false alerts → alert fatigue and missed true incidents
- Blind spots caused by coverage gaps and device downtime → incomplete evidence and reduced trust

These issues are amplified in industrial and remote environments (yards, depots, cross-docks, intermodal points) where backhaul is inconsistent.

Opportunity

Helium IoT can support scalable, decentralized telemetry transport for enterprise monitoring if validated with:

- Sustained packet activity at meaningful scale
- Repeatable deployment and operations processes
- Clear business outcomes tied to incident reduction and operational efficiency

3) Solution Overview

A) NTN-Backhauled Helium IoT Data-Only Hotspot Smart Hub

The Smart Hub will function as a Helium IoT Data-Only Hotspot gateway that:

- Receives LoRaWAN packets from shipment/tote sensor nodes (and/or Smart TOTE-integrated LoRaWAN modules) and site sensors
- Forwards packets into Helium IoT using Semtech Packet Forwarder + Helium gateway software (gateway-rs/helium_gateway) and standard Data-Only Hotspot onboarding
- Uses NTN backhaul in connectivity-constrained locations
- Includes fleet operations capabilities: health telemetry, remote configuration, diagnostics, and uptime reporting

B) Helium-Native AI Risk Monitoring Application (“Smart TOTE Risk Intelligence”)

A production application that:

- Ingests Helium-routed telemetry into an auditable event store
- Normalizes events into a consistent taxonomy (excursion, tamper, route anomaly, connectivity degradation)
- Applies AI to:
 - Risk/anomaly detection (temperature/humidity excursion patterns, tamper signals, route deviation indicators)
 - Alert optimization to reduce false positives while preserving detection performance
 - Predictive maintenance for device health (battery and connectivity reliability)
- Provides: real-time alerts, standardized incident evidence bundles, and operational dashboards

4) Helium-Native Architecture (How This Uses Helium)

This project is designed so that Helium IoT is a core dependency in the telemetry path and in the measurement of success.

Data flow

1. **LoRaWAN endpoints** generate telemetry (temperature, humidity, shock/tilt, door/tamper, battery).
2. **Helium IoT Data-Only Hotspot Smart Hub(s)** receive packets and forward them into Helium IoT.
3. **Helium routing + integration** delivers uplink to the cloud ingestion service.
4. **Event store + normalization** produces an auditable timeline (excursion, tamper, route anomaly, connectivity degradation).
5. **AI Risk Engine** computes risk scores, suppresses duplicates, and prioritizes alerts.

6. **Alerts, dashboards, and incident reports** are produced for operations and customers.

Note on Smart TOTE hardware

The Smart TOTE ecosystem may include BLE sensors and optional gateways for local collection; however, the Helium grant deliverables and KPIs in this proposal are tied to **LoRaWAN endpoints and Helium IoT traffic** (measured by active endpoints, packets, delivery rate, and sustained activity).

5) Why Helium (Helium-Native Justification)

Helium IoT is a core dependency in the architecture:

- The Smart Hub is designed to operate as a Helium IoT Data-Only Hotspot gateway, and telemetry routing is engineered to flow through Helium IoT.
- Project success will be demonstrated through network-meaningful metrics: active gateways, active endpoints, packets forwarded, delivery rate, uptime, and sustained activity windows.
- This project validates decentralized wireless viability for enterprise logistics monitoring under operational constraints (remote sites, harsh environments, and strict incident response needs).

6) Collaboration and Partner Roles (Prospective)

The project is designed for partner collaboration to ensure real-world validation and scale readiness. At the time of submission, the partners below are **prospective**; pilot onboarding outreach is scheduled during M1–M2; LOIs are targeted in 2026.

| Partner | Role | Contribution |
|-----------------------------------|--|---|
| ITracXing (Tracking) | Prime applicant and system integrator | Helium IoT gateway integration, NTN backhaul integration, ingestion pipeline, AI models, alerts/reporting UX, deployment and operations processes |
| Arviem (prospective) | Potential domain and validation collaborator | Logistics workflows, exception taxonomy, chain-of-custody validation methods, international freight use-case alignment (subject to pilot alignment) |
| Vector (3PL / logistics operator) | Potential field pilot and operational validation | Pilot site hosting, acceptance testing, operational workflow validation, |

| Partner | Role | Contribution |
|---|---|--|
| (prospective) | collaborator | measurement of incident response and operational impact (subject to pilot alignment) |
| AT&T (prospective; discussions planned at CES 2026) | Potential enterprise connectivity and benchmarking collaborator | Backhaul benchmarking methodology (terrestrial fallback vs NTN), enterprise deployment best practices, operational readiness input (subject to 2026 partnership discussions) |

Partnership status note: Partners are prospective at submission. Outreach and pilot onboarding discussions are scheduled during M1–M2; LOIs (where appropriate) are targeted in 2026.

Collaboration Governance

- Monthly steering review (milestone readiness, pilot status, risks) once pilot partners are confirmed
- Biweekly execution cadence led by ITracXing
- Formal milestone acceptance checkpoints (pilot readiness, deployment readiness, model validation sign-off, replication readiness)

7) Work Plan, Milestones, and Funding (18 months)

| Milestone | Timeline | Scope of Work | Acceptance Criteria | Funding |
|---|------------|---|--|----------|
| M1 — Architecture and Helium Integration Baseline | Months 1–3 | Finalize hub architecture; Helium IoT Data-Only Hotspot integration baseline; NTN backhaul prototype; telemetry schema; security and device lifecycle | Hub prototype routes test packets via Helium; hub health telemetry visible; lab packet delivery ≥95% | \$50,000 |

| Milestone | Timeline | Scope of Work | Acceptance Criteria | Funding |
|--|-----------------|---|---|----------------|
| M2 — Data Pipeline and MVP Application | Months 4–6 | Helium telemetry ingestion; event normalization; MVP dashboards and alerting; pilot onboarding workflow | End-to-end: Helium packet → event store → dashboard; alerting operational; onboarding workflow ready | \$55,000 |
| M3 — AI Models and Field Pilot Phase 1 | Months 7–10 | Deploy initial hubs/endpoints; train and validate anomaly/risk models; predictive maintenance baseline; incident reporting workflow | Field pilot: ≥5 hubs, ≥300 endpoints; alert F1 ≥0.80; incident reporting workflow live | \$70,000 |
| M4 — Scale Pilot and Reliability Hardening | Months 11–15 | Expand deployments; improve model performance; strengthen operations tooling; reliability/observability hardening | ≥30 hubs active; ≥1,500 endpoints active; hub availability ≥99%; packet delivery ≥97%; alert F1 ≥0.85 | \$45,000 |
| M5 — Production Readiness and Partner Enablement | Months 16–18 | Production hardening; partner enablement; operational readiness for replication; network usage and outcome reporting | Operational onboarding and support processes ready; sustained stable traffic ≥90 consecutive days | \$30,000 |

Total Grant Request: US\$250,000

8) Budget Summary (Use of Funds)

Allocation by category

- **Engineering and product development (60%) — \$150,000**
 - Helium gateway integration, data pipeline, AI modeling, dashboards/alerts, operations tooling
- **Pilot deployment and operations (25%) — \$62,500**
 - Installation, monitoring, partner onboarding, testing, operational validation
- **Hardware prototyping and validation (15%) — \$37,500**
 - Hub iterations, LoRa concentrator/BOM validation, NTN integration test hardware, lab/field validation

Budget is allocated by milestone as defined in Section 7.

9) Quantifiable Positive ROI for the Helium Network

A) Network usage impact (primary ROI)

Targets by Month 15:

- 30 Helium IoT Data-Only Hotspot gateways active (Smart Hubs)
- 1,500 endpoints active (LoRaWAN sensor nodes attached to shipments/totes and/or Smart TOTE-integrated LoRaWAN modules)

Traffic model (planning assumptions for impact reporting):

- Average telemetry rate: 120 packets per endpoint per day
- Daily packets from 1,500 endpoints: 180,000 packets/day
- Packets over a 90-day sustained window: 16,200,000 packets
- Annualized packets: 65,700,000 packets/year

Reporting cadence: Monthly network usage reporting including: active gateways/endpoints, packet throughput, delivery rate, uptime, and sustained activity windows. Where available, we will also report Data Credits consumption from Helium Console exports/invoices (actuals).

B) Ecosystem impact (secondary ROI)

- A repeatable deployment model for sites blocked by traditional backhaul constraints (enabled via NTN)
- Operational readiness that reduces friction for future enterprise onboarding

C) Business outcomes tied to Helium usage

This proposal ties Helium network usage to measurable enterprise outcomes, reported per pilot cohort:

- Incident detection lead time (minutes)
- Temperature excursion severity reduction (degree-minutes) and mitigation time
- False-alert reduction (%), measured as alert precision/recall and F1
- Evidence bundle completeness rate (%) and time-to-claim documentation (minutes)

10) Customer Value and Business Model

Target customers

- 3PLs, freight forwarders, and high-value cargo shippers
- Cold-chain and regulated-product logistics operators
- Industrial yards, ports, and intermodal operators with coverage/backhaul gaps

Value proposition

- Earlier detection of incidents → lower loss severity
- Reduced false alerts → lower operational burden
- Improved continuity → fewer blind spots
- Faster, evidence-ready reporting for compliance and claims workflows

Revenue model

- Subscription per monitored asset / lane / site
- Optional managed deployment and operations service
- Upsells: advanced analytics, automated reporting bundles, predictive maintenance tiers

11) Success Metrics (KPIs)

Helium network KPIs

- Active gateways: ≥ 30 by Month 15
- Active endpoints: $\geq 1,500$ by Month 15
- Packet delivery rate (field): $\geq 97\%$ by Month 15
- Hub availability: $\geq 99\%$ by Month 15
- Sustained activity: ≥ 90 consecutive days by Month 18

Application KPIs

- Alert quality: $F1 \geq 0.85$ by Month 15
- Incident reporting completeness: $\geq 80\%$ of incidents produce complete evidence bundles via a standardized workflow
- Predictive maintenance impact: $\geq 30\%$ reduction in unexpected device downtime versus baseline

12) Execution Capability

ITracXing will execute with a cross-functional team covering:

- IoT/embedded and gateway integration (LoRaWAN gateway + NTN backhaul)
- Cloud data engineering (ingestion, event store, observability)
- ML engineering (anomaly detection, risk scoring, predictive maintenance)
- Product and field operations (deployment, partner onboarding, support)

Key execution roles (planned):

- **Gateway/embedded lead:** Helium IoT Data-Only Hotspot integration, NTN backhaul, device lifecycle/provisioning
- **Data platform lead:** ingestion, event store, observability, and auditability
- **ML lead:** anomaly/risk detection, alert optimization, predictive maintenance
- **Product/ops lead:** alert routing workflows, incident reporting, pilot rollout and partner enablement

Partners contribute domain validation, pilot environments, and benchmarking inputs as defined above.

Sustainability Plan (Post-Grant)

The project is designed to sustain itself after the grant period through:

- **Commercial subscriptions** for monitoring + reporting (tiered pricing by asset count and analytics level)
- **Managed deployment and operations** offerings for enterprise sites (installation, monitoring, SLA support)
- **Partner-led replication** using repeatable onboarding and operations processes to reduce marginal deployment cost

Network Usage Measurement & Reporting

We will provide monthly reporting suitable for Helium Foundation review:

- Active gateways (Smart Hubs), active endpoints, daily/weekly packet throughput
- Packet delivery rate (field) and hub availability
- Sustained activity windows (e.g., continuous 90-day stable traffic)
- Where available, **Data Credits consumption** from Helium Console exports/invoices (actuals)

13) Key Risks and Mitigations

- Gateway onboarding/operational constraints: start Helium gateway integration in M1; implement repeatable provisioning; validate small scale before scaling
- Field variability (RF and installation differences): site survey checklist; remote diagnostics; staged rollout
- Model generalization across lanes: phased deployment; iterative learning; structured acceptance tests with partner validation
- NTN backhaul cost/latency variability: buffer-and-forward design; adaptive sampling policies; terrestrial fallback where available
- Partner readiness/scheduling: defined milestone checkpoints; clear responsibilities and escalation path

14) Foundation Outcomes (What Helium Gains)

Funding this project delivers:

- A practical enterprise proof point for Helium IoT in supply-chain monitoring
- Measurable growth in Helium IoT usage (gateways, endpoints, packets, sustained activity)
- A repeatable deployment model for sites historically constrained by backhaul availability
- A production-ready Helium-native application that demonstrates decentralized wireless viability in real operations