FOUNDATION FOR AI-READY EMERGENCY SERVICES

911 Trust Ledger

The Interoperability Foundation for America’s 911 Data

Jon Whirledge, Founder hello@911trustledger.org www.911trustledger.org

“Interoperability is not the goal. It’s the evidence that the underlying data is trustworthy. One connection. One protocol. One standard of truth.”

240M+
911 calls placed in the US each year

6,000+
PSAPs with no shared data standard

$n^2 \rightarrow n$
Custom integrations replaced by one connection

0
Verifiable cross-system audit trails today

1. The Problem

The 911 Data Ecosystem Is Broken at the Seams

Every major technological shift in 911—analog to digital, wireline to wireless, PSTN to NG911—has added capabilities without resolving the underlying data problem. Emergency communications today is a patchwork of systems that were never designed to share a common vocabulary, verify each other's records, or present a unified picture of what happened during a call.

The result is an ecosystem where interoperability is mostly theater. Agencies claim to interoperate. CAD systems claim to integrate. Standards bodies publish specifications. And yet, when a call transfers between jurisdictions, when a mutual aid request crosses agency boundaries, when an AI system tries to act on 911 data—the data falls apart. The codes don't match. The timestamps conflict. The record is incomplete. And nobody can prove what actually happened.

The n² Integration Problem

The current model for CAD-to-CAD interoperability is bilateral: each agency that wants to share data with another must negotiate a separate integration. Each integration requires its own API contract, schema mapping, authentication mechanism, and maintenance agreement. If you have 10 agencies that need to share data, you need 45 point-to-point connections. If you have 100 agencies, you need 4,950. The math scales as n²—and it fails.

This is not a technology problem. It is an architecture problem. Every bilateral integration is a custom negotiation between two parties who speak different data languages. The cost is paid in staff hours, integration contracts, and failed mutual aid at the worst possible moment.

01

No shared data standard

NENA i3 and EIDO define message formats and transport. They do not define what the data inside those messages means. Every CAD vendor uses different codes for incident types, unit statuses, disposition outcomes, and event classifications. EIDO compliance does not mean EIDO compatibility. Two systems can both be "EIDO compliant" and still be unable to interpret each other's records without a custom translation layer.

02

No verifiable record

Each agency in the 911 chain maintains its own log. No mechanism exists to prove that one party's version of events matches another's. Every audit, every after-action review, every liability dispute starts from scratch—manually reconciling competing logs that were never designed to be reconciled.

03

Non-standard inputs are already here

The 911 data problem is no longer confined to PSAPs and CAD systems. Connected vehicles, building management systems, school security platforms, and autonomous devices are already generating machine-originated calls for service. These sources speak no common dialect. They arrive outside the NENA perimeter with no shared vocabulary, no provenance, and no standard for how their data should be handled.

04

AI is both originating and acting on 911 data

Artificial intelligence is not approaching the 911 ecosystem—it is already inside it. AI systems are triaging calls, generating dispatch recommendations, and in some deployments, initiating contacts with emergency services autonomously. When an AI system both originates a call and acts on the resulting data, and that data has no verified provenance, the downstream decisions are indefensible. There is no chain of custody. There is no audit trail. There is no way to know whether the data was altered, delayed, or misinterpreted in transit.

> *“The question is no longer whether AI will operate inside the 911 ecosystem. It already does. The question is whether the data it acts on can be trusted—and today, it cannot.”*
>
> — Jon Whirledge · Founder, 911 Trust Ledger Foundation

2. Why Existing Approaches Fall Short

Standards Aren’t Enough. Integration Isn’t Enough.

The 911 community has invested heavily in standards, and those investments have delivered real value. NENA i3 provides a modern transport and signaling architecture. EIDO defines a structured envelope for emergency incident data. The industry has made genuine progress toward digitization and interoperability.

But progress toward standards is not the same as solving the underlying problem. The gap is not in the standards themselves—it is in what the standards leave unresolved: semantic meaning, provenance verification, and a shared cross-system truth.

The EIDO Semantic Gap

EIDO defines a standard message structure for emergency incident data. What it cannot define—and does not attempt to define—is what the values inside that structure mean. When Agency A sends an EIDO message with an incident type code of “10-50” and Agency B receives it, nothing in the EIDO standard tells Agency B what “10-50” means. Agency B’s CAD system may interpret it differently, map it to a different dispatch protocol, or flag it as an unknown code entirely.

This is not a flaw in EIDO. It is a reflection of the fundamental challenge: the 911 ecosystem has thousands of agencies that have independently developed local code systems over decades. No standards body can retroactively unify them through a message format specification. What is required is a normalization layer—a mechanism that translates local dialects into a shared semantic vocabulary at the point of data exchange, without requiring any agency to change its internal systems.

Why Bilateral CAD Integration Fails at Scale

The typical response to the interoperability problem has been bilateral CAD-to-CAD API integration: two agencies negotiate a direct connection, map each other’s schemas, and build a bespoke data bridge. This approach works—for two agencies. It does not scale.

Each bilateral integration is a standalone project: scoped, contracted, built, and maintained independently. When an agency changes its CAD system, every bilateral integration must be rebuilt. When a new agency wants to join a regional sharing arrangement, it must negotiate separate integrations with every existing participant. The cost compounds with every new connection. The maintenance burden never ends. And each integration, however well-designed, creates a point of failure that no other party can independently audit.

Challenge	Existing Approach	911TL Advantage

No shared semantic meaning across vendors	EIDO / i3 standards	**Normalization layer converts local codes to a shared canonical vocabulary at ingestion**
Point-to-point integrations scale as n^2	Bilateral CAD API contracts	**One 911TL connection replaces custom integrations between every pair of agencies**
No verifiable record across system boundaries	Centralized logging	**Distributed, tamper-evident ledger maintained by all participants**
Non-standard inputs have no defined ingestion path	None	**Canonical registry handles any source that can produce a structured event**
AI acting on unverified data creates indefensible decisions	None	**Every event carries cryptographic provenance—origin, timing, and chain of custody proven**

3. The Solution

One Connection. One Protocol. One Standard of Truth.

The 911 Trust Ledger Foundation (911TL) builds the protocol layer that resolves all three failures simultaneously: semantic normalization, verifiable provenance, and scalable interoperability through a single shared connection instead of bilateral integrations.

911TL is not a CAD system. It is not a routing platform. It does not move calls or replace any component in the existing 911 stack. It functions as a read-only subscriber to existing event streams—a permanent, tamper-evident record of what happened, anchored to a shared semantic vocabulary that every participant can trust.

Three Layers. One Pipeline.

A vendor or agency connects their event stream to 911TL once. That single passive connection simultaneously powers three integrated layers.

Layer 1 — Trust Layer	Layer 2 — Data Layer	Layer 3 — Economic Layer
Every critical event generates a cryptographic proof: a hash of the event data plus digital signatures from the originating systems. These proofs are stored on a permissioned Hyperledger Fabric ledger maintained by all network participants. No single party controls it. No record can be altered without detection by every other participant.	From the same event stream, the Event Normalizer produces structured, PII-free records in a canonical vocabulary shared across all participants. Local codes are mapped to standard definitions at ingestion. The result is a record that any participant can interpret—regardless of their CAD vendor or internal coding system.	Participants who contribute normalized event records to the shared data commons earn rewards proportional to their contributions. AI companies and analytics consumers pay licensing fees to access the commons. Those fees fund Foundation operations and distribution back to contributors.

The Semantic Normalization Layer

The Data Layer’s normalization function is where 911TL directly resolves the interoperability problem that standards alone cannot solve. Every CAD vendor maintains its own internal codes for incident type, unit status, disposition outcome, and resource classification. These codes are meaningful within each system—and meaningless outside it.

911TL’s Event Normalizer maintains a canonical registry that maps every known vendor’s local codes to a shared semantic vocabulary. When an event record enters the 911TL pipeline, local codes are translated to canonical values before the record is written to the data store. The original values are preserved in the Trust Layer proof. The normalized values are what participating agencies share.

The practical result: when Agency A's CAD system dispatches a "Traffic Accident with Injuries" using code "10-50I," and Agency B's CAD system uses "MV Crash, Injury" for the same event type, both records arrive in the shared commons with the same canonical incident classification. No custom translation layer. No bilateral negotiation. No bespoke schema mapping.

> *"One 911TL connection replaces the custom integration that would otherwise have to be built between every pair of agencies in a region. The math goes from n^2 to n."*
>
> — Jon Whirledge · Founder, 911 Trust Ledger Foundation

Non-Standard Inputs

The 911 data perimeter has already been breached. Connected vehicles initiate automatic crash notifications. Building management systems trigger alarms. School security platforms generate lockdown events. Autonomous devices call for service with no human in the loop. These sources do not conform to NENA standards because they were never built within the NENA ecosystem.

911TL addresses this through the canonical registry: a defined ingestion path for any source that can produce a structured event. Sources outside the standard stack connect through a documented submission protocol, declare their event types against the canonical taxonomy, and receive the same normalization treatment as native i3 sources. Their records are provenance-anchored, semantically normalized, and verifiable—indistinguishable in the commons from records produced by a fully i3-compliant ESInet.

4. How It Works

Five Steps. One Passive Connection.

The 911TL pipeline integrates with zero disruption to existing operations. 911TL never touches a call. It never modifies any ESInet component. It observes, records, and normalizes—as a read-only downstream subscriber.

01

Connect

A participating vendor or agency connects their event stream to the 911TL passive subscriber. For ESInet environments, the subscriber attaches to existing NENA i3 log streams across BCF, ECRF, LVF, and CHE functional elements as a read-only downstream consumer. No upstream impact. No modification to existing systems. For non-ESInet sources—CAD direct, connected devices, non-standard inputs—a documented submission protocol defines the ingestion path.

02

Generate Proof

From each event record, the Proof Constructor generates a cryptographic fingerprint: a hash of the event data plus digital signatures from the originating components. Cross-hop linkage pointers chain each proof to the prior hop in the event path, forming a verifiable chain of custody from first trigger to final disposition. This proof is stored in the Trust Layer—immutable, participant-verified, and tamper-evident.

03

Normalize

The Event Normalizer processes the same event record and translates all local codes to canonical definitions using the 911TL canonical registry. Identity-bearing and location-bearing fields are transformed at the point of processing: ANI becomes a call category, precise location becomes a jurisdiction code, caller identity becomes anonymized metadata. The normalized record carries full operational meaning without carrying personal data.

04

Store Locally

Both outputs—the cryptographic proof and the normalized event record—are stored in the participant's own infrastructure. The participant has immediate access to both for their own operational analytics, quality improvement, and compliance use. The data physically lives with the participant. "Your data never leaves your control" is a technical fact, not a policy promise.

05

Share (Optional)

Through the Contribution Manager, participants choose whether to contribute their normalized records to the shared data commons, which event types to include, and under what terms access is granted. Every query against their data is visible to them. They can adjust or withdraw at any time. Sovereignty is structural, not procedural.

ESInet Integration: How the Binding Works

For ESInet environments, 911TL uses a lightweight SIP header to bind the operational call record to the ledger transaction without either system doing the other's job. A structured header (X-911TL-Ref or Call-Info) carries the ledger transaction reference in SIP signaling, creating a durable link between the call in the ESInet and the proof record in the ledger. The two systems remain independent—the header is the bridge.

For environments where SIP signaling is unavailable, Hyperledger Fabric block event subscription serves as the floor: the ledger's own event stream provides the binding mechanism without requiring any changes to the operational network. This ensures that 911TL integration is achievable in any deployment context, including legacy environments that have not yet completed NG911 migration.

5. Governance & Neutrality

Community-Governed. Vendor-Agnostic. Open Protocol.

The value of a shared protocol layer depends entirely on its neutrality. A trust infrastructure that any single vendor, agency, or government entity can capture is not trust infrastructure—it is a competitive moat with a neutral-sounding name.

911TL is governed as a foundation: a neutral nonprofit steward accountable to the community it serves, not to any commercial interest. The governance model is explicitly modeled on the institutions that have built the most durable technology commons in history.

Foundation Governance Sets participation rules, privacy policy, consensus policy, and economic framework. Governed by the membership—PSAPs, ESInet operators, carriers, vendors, and state authorities. No single member holds veto power.	**Technology Stewardship** Maintains the open-source Hyperledger Fabric codebase, documentation, and canonical registry. The protocol is Apache 2.0 licensed. No protocol licensing fees. Any vendor can build on it without permission or cost.	**Access Brokerage** Operates the federated query layer through which AI companies and analytics consumers access the data commons. Enforces licensing terms. Distributes rewards to contributors. Never holds data centrally.
Role Separation CAD vendors are canonical registry contributors and native integration owners. Integrators own deployment, managed services, and regional channel architecture. The Foundation governs the protocol—it owns neither.	**Standards Alignment** Designed to complement NENA i3, EIDO, NIEM, EDXL, and Project 25—not compete with them. Every integration point anchors to an existing standard. Where 911TL specifications mature, they are offered for standardization consideration.	**MOU Enforcement** Inter-agency data sharing governance maps onto existing MOU practice—rendered as executable ledger objects enforced by chaincode. Existing agreements become auditable, enforceable technical policy. No new governance frameworks required.

Analogues in Infrastructure

The IETF governs TCP/IP. The Linux Foundation governs Hyperledger Fabric. The Apache Software Foundation governs the open-source stack that runs most of the world’s servers. Each governs a protocol—not a product. Each is funded by the commercial ecosystem that benefits from the protocol’s existence, not by controlling access to the protocol itself.

911TL occupies the same structural position in the emergency communications ecosystem. The protocol is the public good. The commercial ecosystem—CAD vendors, integrators, AI companies—builds on it. The Foundation governs it in the interest of the community it serves.

6. Data Provenance & AI Safety

AI Cannot Be Trusted Without Provenance. Neither Can 911.

The urgency of the 911 data problem is not hypothetical. Artificial intelligence is already operating inside the emergency communications ecosystem. Predictive dispatch systems are recommending resource allocation. AI triage tools are classifying incoming calls. Automated alert systems are generating contacts with PSAPs without any human in the loop.

Each of these applications depends on data. And in every case, that data currently arrives without any verifiable chain of custody. There is no mechanism to prove that the data an AI system is acting on has not been altered, delayed, fabricated, or misrouted since it was generated. The AI system must trust its inputs—and has no technical basis for doing so.

The Indefensible Decision Problem

Consider a connected vehicle that automatically reports a high-speed collision to 911. An AI triage system classifies the event as high-priority and routes it for immediate dispatch. First responders arrive and find no collision. The vehicle's location data was incorrect. The AI's classification was based on a fabricated or corrupted input. Resources were diverted from a genuine emergency.

Who is responsible? The vehicle manufacturer? The ESInet operator? The PSAP? The AI vendor? Without a verifiable provenance record—a tamper-evident log of where that data came from, when it entered the system, which components handled it, and what it contained at each step—there is no answer. The decision is indefensible not because anyone behaved negligently, but because the infrastructure does not exist to produce a defense.

This is the problem 911TL solves. Every event that passes through the 911TL pipeline carries a cryptographic proof of its origin and its chain of custody. When an AI system acts on a 911 event, the proof exists. When a question arises, the record answers it. The decision is defensible.

> *"When AI is both originating and acting on 911 data, the absence of verified provenance is not a technical inconvenience. It is a systemic liability for every organization in the chain."*
>
> — Jon Whirledge · Founder, 911 Trust Ledger Foundation

The AI Data Commons

Beyond provenance, 911TL creates the data substrate that responsible AI in public safety requires. The shared data commons—built from normalized, PII-free event records contributed by participating agencies—is the only cross-jurisdictional, verified, AI-ready dataset covering the operational reality of emergency response in the United States.

This dataset does not exist anywhere today. Not in any government database. Not in any vendor's data lake. Not in any research archive. It is created as a byproduct of infrastructure that participating agencies are already deploying for the Trust Layer and interoperability functions. The AI commons is not an add-on—it is what happens when the interoperability problem is solved correctly.

7. Who We Work With

Built for Everyone in the NG911 Ecosystem.

911TL is designed as a protocol layer—which means its value flows to every participant in the ecosystem that depends on trustworthy data. The architecture deliberately separates roles: the Foundation governs the protocol; CAD vendors and integrators own the commercial deployment; PSAPs and state authorities maintain sovereignty over their data.

CAD Vendors & Integrators

Connect your event stream once. Deliver verifiable data integrity and semantic interoperability to your customers. Replace bespoke bilateral integrations with a single standard connection. Earn rewards for validator participation. Build on open APIs.

PSAPs & State 911 Authorities

Deploy the Trust Layer as compliance infrastructure. Keep your data in your own systems—always. Use your normalized local data store for operational analytics. Earn rewards by contributing to the commons on your own terms. Replace bilateral MOUs with enforceable ledger governance.

ESInet Operators & Carriers

Deliver verifiable chain of custody across the ESInet without modifying any functional element. Reduce audit overhead. Demonstrate system performance with tamper-evident records. Support multi-jurisdiction interoperability without bespoke integration contracts.

AI & Technology Companies

Access a verified, normalized, cross-jurisdictional dataset that doesn't exist anywhere else. Build models on data with cryptographic provenance. Meet regulatory and compliance expectations for AI in public safety. License access through a single Foundation API.

Standards Bodies & Regulators

A community-governed, open-protocol approach that extends NENA i3 and aligns with NG911 modernization objectives. A neutral infrastructure layer that no single vendor or agency controls. A path for 911TL-native specifications to inform future standards.

Research & Academic Partners

A verified, longitudinal dataset of emergency response operations at national scale—available through licensed access. The foundation for evidence-based public safety policy, AI safety research, and system performance benchmarking.

8. Implementation & Roadmap

From Protocol to Ecosystem.

911TL is being built incrementally, with each phase delivering immediate operational value while laying the foundation for the next. The go-to-market sequence is designed around the problems agencies are already trying to solve—CAD-to-CAD interoperability, after-action audit capability, and normalized data for analytics—with the trust layer and AI commons as enabling substrate, not a precondition.

Phase 1

Core Infrastructure & First Deployment

Launch the Trust Layer on Hyperledger Fabric 2.5 LTS. Demonstrate event notarization in a live CAD-to-CAD interoperability deployment. Establish the Foundation governance framework. Deploy the local data store alongside the node software. Publish the canonical registry as an open specification.

Phase 2

Semantic Normalization & Regional Expansion

Activate the Event Normalizer and Contribution Manager. Onboard founding agencies and CAD vendors as canonical registry contributors. Demonstrate cross-agency event normalization: same incident, different CAD vendors, identical canonical record. Expand to anchor state 911 authority as first large-scale institutional partner.

Phase 3

Data Commons & Economic Layer

Activate the federated query brokerage and launch the licensed data commons. Onboard initial AI and analytics consumers. Demonstrate the economic flywheel: contribution drives value, value drives licensing revenue, revenue drives rewards, rewards drive contribution. Publish normalized event schema as an open standard.

Phase 4

National Scale & Standards Engagement

Expand participation nationally. Engage NENA, APCO, and standards bodies with 911TL-native specifications for potential standardization consideration. Grow the AI ecosystem built on the commons. Every new participant strengthens the network; every improvement contributes to the public good.

The Sequence Logic

CAD-to-CAD interoperability is the entry point—not because it is the largest problem, but because it is the most immediate, and because it produces the infrastructure that solves everything else. An agency that deploys 911TL for regional CAD interoperability automatically gets the Trust Layer, the normalized data store, and the connection to the commons. The interoperability win is the on-ramp.

9. Conclusion

The Proof Beneath the Promise.

The 911 data problem is not new. It has accumulated over decades of independent development, bilateral negotiation, and point-to-point integration. It cannot be solved by another standard, another API contract, or another bilateral agreement. It requires a protocol layer—a shared foundation that every participant connects to once, that normalizes the data, verifies its provenance, and makes every connection in the ecosystem stronger for every new participant that joins.

That is what 911TL builds. Not a product. Not a platform. A protocol—open, vendor-agnostic, community-governed, and designed to become as invisible and indispensable as the infrastructure it sits beneath.

The interoperability problem is solvable. The semantic normalization problem is solvable. The provenance problem is solvable. The AI safety problem in emergency communications is solvable. The solution to all of them is the same architecture. And it is available today.

> *“Public safety runs on trust. 911TL makes that trust verifiable, interoperable, AI-ready, and economically self-sustaining.”*
>
> — Jon Whirledge · Founder, 911 Trust Ledger Foundation

Get Involved

hello@911trustledger.org

www.911trustledger.org