

RFP 27-88426: Fleet GPS / Telematics Services Statement of Work

1. Executive Summary

The Indiana Department of Administration (IDOA), on behalf of participating State agencies, seeks to procure a turnkey, enterprise-grade Fleet Telematics and GPS Tracking solution capable of supporting Indiana's statewide vehicle fleet. The State strongly prefers a secure, reliable, and scalable cloud-based service offering. Cloud-based service offerings are required to be within a state-owned cloud tenant. However alternative solutions may be considered if they demonstrate significant value. This section provides details on infrastructure and support requirements, outlining the State's minimum requirements. Review and completed Attachment M – Infrastructure Overview for more detailed information.

The State requires an integrated system that unifies real-time vehicle location data, diagnostic telemetry, and driver behavior insights within a single operating environment accessible to all participating agencies. This initiative is intended to modernize fleet oversight by improving operational visibility, enhancing safety, and reducing total cost of ownership (TCO).

The selected Contractor ("Vendor") shall provide:

- Cellular-enabled GPS tracking hardware.
- A web-based, intuitive telematics software platform.
- Ongoing Maintenance, and technical support services.
- Compliant, secure data retention and archiving.
- Comprehensive user and administrator training.

While innovative and value-added capabilities are welcomed, all proposed solutions must, at a minimum, meet the State's defined technical, operational, and security requirements to ensure long-term compatibility with established state procurement and technology standards.

2. Background and Current State

Historically, GPS tracking has been deployed fragmentedly across select state agencies, resulting in inconsistent reporting practices and limited central visibility of State assets. The legacy telematics environment presented significant operational challenges, including:

- Inaccurate and unreliable reporting within the web-based tracking platform.
- Substandard hardware behavior that triggered excessive wireless update cycles, leading to critical battery drain on stationary state vehicles.

To resolve these deficiencies, the State intends to establish a standardized GPS/telematics utility capable of delivering high-accuracy reporting, stable, fit-for-purpose hardware, and simplified enterprise administration.

State Fleet Inventory Profile (Approximate)

The following profile represents the State's current baseline fleet distribution across participating agencies:

Participating Agency	Approximate Vehicle Count & Type
Indiana Department of Administration (IDOA)	140 vehicles
Indiana Department of Transportation (INDOT)	3,471 vehicles
Department of Natural Resources (DNR)	1,200 fleet vehicles / 250 law enforcement vehicles
Department of Correction (DOC)	640 fleet vehicles
Indiana State Police (ISP)	2,064 vehicles
TOTAL ESTIMATED FLEET	7,725 vehicles

3. Scope of Work

3.1 System Functional Requirements

The platform must provide a comprehensive, secure, and intuitive graphical user interface (GUI) allowing authorized personnel to view, manage, and analyze assigned fleet assets in real time.

- **Real-Time Tracking & Playback:** The core system must display live vehicle locations on a dynamic, high-resolution GIS map, capture movement history, and provide detailed route playback. This functionality must support day-to-day dispatch, after-action analysis, incident review, and strategic operational planning. See the Geo-Spatial Data and Services Integration below.
- **Vehicle Diagnostics & Health:** The platform must ingest and process telematics data including vehicle health indicators, basic onboard diagnostics (OBD), Diagnostic Trouble Codes (DTCs), odometer readings, and fuel consumption rates. The battery draw of the installed devices must meet OEM minimum requirements. The speed of the vehicle must come from the ECM directly and not

calculated by an algorithm. The system must aggregate this data to enable proactive preventative maintenance planning and risk mitigation.

- **Driver Behavior & Safety Coaching:** To support performance and accountability, the solution must analyze driver behavior metrics (e.g., speeding, harsh braking, rapid acceleration, excessive idling, and unsafe maneuvers) and synthesize these data points into actionable driver safety scores and report cards.
- **Geofencing & Alerts:** The platform must support user-defined geofencing, allowing agency administrators to establish virtual spatial boundaries and receive automated, near-instantaneous alerts (via email/SMS/system notification) upon vehicle entry or exit.
- **Reporting & Configuration:** The software must support configurable dashboards, configurable reports, and alerts tailored to individual agency workflows.

Minimum System Functional Requirements Summary:

- Real-time GPS visibility and tracking
- Historical route playback and pathing logs
- Integrated diagnostic data and fault code (DTC) reporting
- Fuel usage tracking and fuel efficiency analytics
- Driver behavior monitoring, profiling, and safety scoring
- Configurable geofencing with automated, rule-based alerts
- Must have capability to integrate with dump truck hydraulics or chassis system to read salt distribution data both in real time and historical.
- Customizable and exportable reporting formats (PDF, CSV, Excel)
- Secure web browser and mobile device accessibility

3.2 Hardware & Telematics Device Requirements

To ensure the integrity of the collected telematics data, the Contractor must provide durable, secure, and highly compatible hardware capable of supporting a diverse, multi-class state fleet. This includes light-duty, heavy-duty, specialty vocational equipment, and off-road assets.

- **Installation & Deployment:** Devices must be simple to install and automatically transmit high-fidelity telemetry data under varying environmental and operational conditions without disrupting the host vehicle's electrical or mechanical systems.
- **Diagnostics Port Integration:** Hardware must securely interface with standard onboard diagnostics interfaces, including OBD-II, RP-1226, or OEM-embedded telematics systems.
- **Firmware & Connectivity:** Devices must support over-the-air (OTA) firmware updates without interrupting live tracking or risking data loss. Given the State's varied terrain, the hardware must utilize reliable cellular networks with automatic secondary carrier/pathway failover and offline caching capabilities to store data when connectivity is lost.

- **Tamper Protection & Energy Management:** To safeguard state assets, devices must feature integrated tamper detection and alert mechanics (e.g., unauthorized disconnection alerts). The hardware must also incorporate smart power management to prevent auxiliary battery drain on inactive vehicles.

Minimum Hardware Requirements Summary:

- Broad compatibility with OBD-II, J1939, and/or OEM embedded telematics systems
- Ruggedized, hermetically sealed, and tamper-resistant device construction
- Secure, end-to-end encrypted data transmission (device-to-cloud)
- Multi-carrier cellular connectivity with automatic fallback and local offline caching
- Support for seamless, over-the-air (OTA) firmware and configuration updates
- Advanced low-power sleep modes to guarantee battery draw protection

3.3 Security & Compliance Requirements

The proposed solution must strictly adhere to rigorous security frameworks consistent with State policy, statutory data protection mandates, and statewide procurement technology standards.

- **Encryption & Access Control:** The platform must secure data-in-transit and data-at-rest utilizing industry-standard encryption protocols. User access must be governed by a Role-Based Access Control (RBAC) framework to restrict data visibility based on agency hierarchy and job function.
- **Audit Logging:** The system must generate immutable, comprehensive audit logs tracking user logins, configuration modifications, administrative changes, and data exports.
- **Data Retention:** The system must maintain a minimum of 365 days of online, immediately accessible telematics data, with a clear process for retrieving long-term archived records upon request.
 - The State is the sole owner of all telematics data, metadata, logs, derived analytics, and configurations. Vendor receives a limited, non-exclusive license to process the data solely to provide services under this Contract. No secondary use (e.g., model training, resale, benchmarking) is permitted without prior written approval.
 - Vendor is entirely responsible for storing and managing the data. Data storage will not be managed by State agencies

Minimum Security Requirements Summary:

- Industry-standard encryption algorithms for data-in-transit and data-at-rest
- Granular Role-Based Access Control (RBAC) with single sign-on (SSO) compatibility
- Comprehensive administrative, system, and user audit logging

- Strict compliance with Indiana Office of Technology (IOT) cybersecurity, hosting, and retention policies
- Minimum of 365 days of active online data availability with reliable long-term archiving solutions

3.4 Integration & Interoperability Requirements

The State's long-term fleet management strategy relies on enterprise interoperability and the elimination of isolated data silos.

- **API Availability:** The selected system must support secure integration with existing State fleet and financial management systems. See Data Exchange under the Compliance Requirement section.
- **Workflow Interoperability:** Systems must operate cohesively to push maintenance alerts, fault code notifications, and critical diagnostic warnings directly into state work order systems or external agency communication tools to ensure rapid response and unified financial oversight.
- **Geo-Spatial Data and Services Integration**
 - The State of Indiana utilizes an ESRI-based Geographic Information System as the authoritative source for geo-spatial data.
 - The solution must enable seamless integration with an existing ESRI-based SaaS and enterprise GIS platform, as mutually agreed upon, which serves as the definitive source for spatial data statewide.
 - The proposed solution is required to deliver integrated GIS mapping functionality. This includes demonstrating the capability to interface with current ESRI (ArcGIS) environments, consume ESRI map services, support ESRI data formats, maintain synchronization with agency-managed GIS datasets, and uphold location validation processes presently facilitated by ESRI-managed map data and services.
 - If the proposed solution does not natively utilize ESRI technology, the respondent must provide a detailed explanation of how interoperability with the State's ESRI-based GIS environment will be accomplished. This description should address how location validation functionality will be sustained, and outline any necessary middleware, data translation procedures, or additional licensing requirements.

Minimum Integration Requirements Summary:

- Secure, robust, and fully documented RESTful APIs (or equivalent)
- API will be deliverable by various attributes, including datetime, either range or single timestamp, and VIN
- API will have two endpoints: one to retrieve historical data and one to retrieve live data
- Compatibility with State fleet management and ERP financial systems
- Extensible architecture capable of supporting future system integrations

- Data extraction and export capabilities utilizing common, non-proprietary formats (e.g., JSON, XML, CSV), with agency-provided documentation detailing the variables currently tracked, including definitions, naming conventions, and historical context for each data element.
- Seamless workflow integration pushing real-time alerts and maintenance events to designated external systems

4. Objectives of Engagement

The overarching goal of this partnership is to implement a unified, modern GPS tracking and telematics framework that strengthens fleet management, maintenance, and administrative oversight across the State of Indiana.

The primary objectives include:

1. **Real-Time Fleet Visibility:** Deliver highly accurate, reliable, real-time data regarding vehicle location, movement, and utilization.
2. **Enhanced Safety & Accountability:** Strengthen driver safety, reduce liability, and increase accountability through objective, behavior-based coaching and analysis.
3. **System Consolidation:** Eliminate operational fragmentation by migrating individual agency efforts into a single, scalable, statewide telematics portal.
4. **Secure, Audit-Ready Data:** Maintain a highly secure data repository with granular access controls and compliant retention to support state audits and performance reviews.
5. **Standardized Fleet Analytics:** Enable standardized reporting to drive strategic planning, capital budgeting, lifecycle analysis, and administrative oversight.
6. **Future-Readiness:** Ensure long-term viability through an open, flexible architecture capable of integrating with emerging automotive and fleet management technologies.

5. Deliverables

5.1 Deliverable Categories

The Contractor shall perform and provide the deliverables specified below, adhering to the quality standards established by the State:

- **GPS Hardware & System Setup:** Furnish and install all required GPS tracking hardware, wiring harnesses, and mounting accessories with negligible disruption to active state operations. The Contractor must collaborate on centralized installation hubs and/or deploy mobile technicians to individual state agency locations. Standardized installation/removal procedures and commissioning/decommissioning configuration documentation must be provided.

- **Software/Interface Deployment:** Deliver a fully operational, cloud-hosted, web-based software platform featuring administrative, agency-level, and user-level access tiers. Enable full remote configuration capabilities (e.g., ping rate tuning, geofence mapping, alert thresholds, power management settings) and robust data export options (CSV, PDF, DOCX).
- **Training Materials & Sessions:** Design and execute instructor-led training tailored to IDOA and individual agency workflows, accommodating 10 to 25 participants per session. Provide comprehensive digital training materials, quick reference guides, and subsequent training sessions aligned with major software updates.
- **Reporting & Documentation:** Deliver comprehensive documentation including data retention and backup plans, system configuration guides, customer support channels, escalation procedures, and service-level agreement (SLA) performance matrices.

5.2 Baseline Project Schedule

IDOA expects the Contractor to adhere to the following baseline implementation timeline:

#	Task / Milestone	Contractual Due Date
1	Initial Project Kick-off Meeting	Scheduled within five (5) business days of contract award; executed within thirty (30) calendar days.
2	Strategic Project Plan Delivery <i>(Review, evaluate, adapt, and improve)</i>	Submitted within ten (10) business days following the Kick-off Meeting.
3	Initiation of Hardware Installation & Software Deployment	Commenced within fifteen (15) business days following the Kick-off Meeting.
4	Hardware Installation & System Deployment Completion	Concluded within forty-five (45) business days following the Kick-off Meeting.
5	Recurring Monthly Status & Performance Reporting	Submitted monthly or by request.

6. Payment Milestones

IDOA will structure progress and operational payments to align directly with verified, completed deliverables, including but not limited to:

- Successful delivery, provisioning, and acceptance of physical hardware.
- Verified deployment, testing, and operational readiness of the software platform.
- Completion and acceptance of training sessions and technical documentation.
- Recurring monthly subscription, hosting, and software licensing fees.
- Structured recurring maintenance and support service payments.

7. Project Management

7.2 Project Management Plan

The Contractor shall deliver an initial draft of the Project Management Plan (PMP) within 30 business days of contract start. A comprehensive PMP will be delivered at a mutually agreed upon timeframe. Final acceptance of the PMP is defined in the deliverables section. The PMP will include an integrated schedule with milestones and dependencies; a project organization and staffing plan; a requirements traceability matrix; issue and risk management processes with escalation paths; a communication plan for stakeholder engagement; a quality management plan with standards and acceptance criteria; training and deployment plans; and descriptions of approved tools and collaboration platforms. The PMP shall include a change control process to evaluate and approve scope changes. The PMP will be reviewed and approved by the State and updated as necessary.

7.3 Key Persons

The following individuals are designated as key persons for this engagement:

- Project Manager: Responsible for overall project coordination, schedule management, and communication with the State.
- Technical Lead: Responsible for solution design, technical oversight, and integration activities.

Individuals designated for these roles will be appointed during the development of the PMP. Any substitution of key persons must be approved in writing by the State. The Contractor shall ensure that any proposed replacement meets or exceeds the qualifications of the originally designated individual. The State reserves the right to request the replacement of any key person if, in the State's judgment, the individual does not meet performance expectations or project needs. Additionally, the State shall have the opportunity to interview any proposed replacement prior to approval to ensure suitability for the role.

7.1 Project Governance Roles

- **Contractor Project Manager:** The Contractor must assign a dedicated Project Manager responsible for coordinating all implementation efforts, schedules, communication, training, and technical escalation pathways.
- **IDOA Contract Manager:** IDOA will assign a Contract Manager to oversee contract compliance, facilitate inter-agency coordination, and review/approve project deliverables.

7.2 Other Project Staff

The Contractor shall provide sufficient staffing levels with appropriate qualifications to meet the State's delivery timelines and performance expectations. The Contractor shall prepare a Project Resource Staffing Plan that includes:

- The number, type, and categories of staff proposed for the engagement.
- Role descriptions and minimum qualifications for each position.
- Work location details and any remote work arrangements.
- Ongoing training requirements to ensure compliance and quality standards.
- A plan for onboarding new staff or replacing personnel during the engagement.

The State reserves the right to review staffing and to request changes if, in the State's judgment, personnel do not meet performance expectations or project needs. The State will have the opportunity to interview proposed replacements prior to approval, and any replacements must meet or exceed the original qualifications.

7.3 Document Management

The State will establish an electronic project library using SharePoint as the primary repository for all deliverables and administrative documents. The Contractor shall submit documents in editable and PDF formats, apply State-approved naming conventions, and maintain version control with an audit trail. Access permissions will be managed by the State to ensure confidentiality and compliance with applicable security and privacy standards.

7.4 Status Updates and Performance Reporting

The Contractor shall provide recurring progress updates, including:

- Installation, commissioning, and deployment progress metrics.
- Monthly platform service performance and uptime reports.
- System outage, latency, and security incident reports.
- Active hardware inventory records, failure rates, and warranty replacement cycles.

8. Compliance Requirements

The Contractor must maintain strict, verifiable compliance throughout the contract lifecycle with:

- **Statewide IT Policies, Procedures, & Standards:**

The State has robust and comprehensive security standards that permeate all levels of the organization. The Indiana Office of Technology (IOT) has been tasked with establishing and maintaining these security standards. The security standards include assessing security risks, developing, and implementing effective security procedures, and monitoring the effectiveness of those procedures. If the proposed solution involves information technology-related products or services, all such products or services are to be compatible with any of the technology standards found in the [Statewide IT Policies, Procedures, & Standards](https://www.in.gov/iot/policies-procedures-and-standards/) (<https://www.in.gov/iot/policies-procedures-and-standards/>) that are applicable, including the assistive technology standard. The Contractor will be required to sign a Non-Disclosure Agreement (NDA) to access the more sensitive standards and policies. The Contractor should review the Statewide IT Policies, Procedures, & Standards and ensure their proposed solution meets all standards therein.

- **Data Exchange:** The State has robust and comprehensive data transmission standards that operate enterprise wide. The IOT established and maintains these standards, which support IOT's data exchange and API-led strategies for the State. The Contractor's solution must support the State's standard API and file transfer methods to facilitate secure data transmission. The State's standardized data transmission technologies are the MuleSoft API Management and GoAnywhere Managed File Transfer (MFT) services. See <https://www.in.gov/iot/policies-procedures-and-standards/applications-standards/>.
- **Authentication:** The proposed solution is expected to integrate with Access Indiana. The IN.gov Program (<https://www.in.gov/inwp/>) is tasked with implementing a single sign-on authentication mechanism and Identity Provider for online applications for the State of Indiana, referred to as Access Indiana. The benefits of a standard authentication solution, integration strategy, integration process, and more can be found at Access Indiana Authentication (<https://www.in.gov/inwp/applications/authentication/>).
- **Artificial Intelligence Standards:** The State maintains an enterprise AI Policy overseen by the Office of the Chief Data Officer (OCDO), in coordination with the Chief Privacy Officer (CPO) and the Management Performance Hub (MPH). Any solution containing AI or machine-learning functionality must comply with this policy and complete the State's AI Readiness Assessment Process, including submission and approval of the Readiness Assessment Questionnaire, before the AI capability can be implemented or used. Additional information is available at <https://www.in.gov/mph/AI/>.

- **Data Privacy & Encryption:** Strict compliance with State-mandated data privacy rules, utilizing robust encryption algorithms for all data-at-rest and data-in-transit.
- **Incident Response & Audit Logging:** Mandatory compliance with state-level incident reporting timelines, disaster recovery protocols, and immutable audit log preservation.
- **Statutory Compliance:** Adherence to all applicable Federal and State of Indiana laws, regulations, and administrative guidelines.

9. Key Performance Indicators (KPIs)

The State will utilize a set of Key Performance Indicators (KPIs) to monitor, measure, and score the Contractor's performance. Specific KPI targets and metrics will be mutually finalized prior to contract finalization, but must include, at a minimum:

- **System Uptime & Platform Responsiveness**
- **GPS Tracking & Location Accuracy**
- **Device Reporting Reliability** (*e.g., ping frequency, geofencing execution, stop report logging*)
- **Technical Support Responsiveness** (*e.g., ticket triage, response time, and mean time to resolution*)
- **Data Retention Integrity & Export Availability**
- **User Satisfaction Metrics**

The State will measure on-time delivery of the scope of work, adherence to quality standards, and budget compliance. Additionally, the State reserves the right to collect a modified Net Promoter Score from state agency users.

Contractual Default Threshold: Substandard ratings on the modified Net Promoter Score, or a persistent failure to meet any other agreed-upon KPI targets, may be deemed, at the sole discretion of the State, to constitute a material default under the Contract.

10. End of Contract Transition and Turnover

The Contractor shall develop a turnover plan six months prior to contract end, detailing activities for transferring responsibilities, non-proprietary components, data, and operational documentation to the State or its agent. The Contractor shall maintain mutually agreed upon staffing levels during turnover and commence training and shadowing six months prior to contract end for staff who will assume operations. The State will approve the designated Turnover Manager. The Contractor shall provide a knowledge transfer checklist (for example procedures, contacts, training materials) and deliver a data disposition certificate confirming deletion or return of State data within six months of contract completion unless otherwise agreed.