

ATTACHMENT A

SCOPE OF WORK

1 PURPOSE

To provide Customers with Telematic Asset Tracking Services and Related Equipment, on a statewide basis, pursuant to the terms set forth in this Scope of Work.

2 DEFINITIONS

Definitions contained in section 287.012, Florida Statutes (F.S.); Rule 60A-1.001, Florida Administrative Code (F.A.C.); and Attachment E, Enterprise Standard Terms and Conditions; are incorporated by reference. In the event of a conflict, the definitions listed in this section supersede the incorporated definitions for the purposes of this Scope of Work. All definitions apply in both their singular and plural sense.

Add-On Services and Related Equipment (Optional) – Non-core or additional services available for purchase to enhance or support the Telematic Asset Tracking Services and Related Equipment solution.

Application Programming Interface (API) – A documented interface that enables authorized systems, devices, and applications to securely exchange Customer Data through automated transactions, bulk transfers, or event-based communications.

Asset – A State-owned or leased motor vehicle, equipment, or other trackable Asset intended to be monitored under a purchase off the Term Contract.

Business Day – Monday through Friday, inclusive, except for those holidays specified in section 110.117, F.S., from 8:00 a.m. to 5:00 p.m. at the Customer's location.

Cloud Software (SaaS) – A web-based platform where users can perform the following, including but not limited to: view maps, track Assets, create Geofences, generate reports, and manage alerts.

Commodity – As defined in section 287.012, F.S. May be used interchangeably with "related equipment."

Connectivity – Cellular, satellite, or other communications service, including required carrier plans, that transmits data between Hardware and the hosted solution.

Contract Manager – The representative designated by the Department who will oversee all aspects of the Term Contract, monitor performance expectations, and serve as the primary point of contact for the Contractor.

Contracted-Professional Service Rate – The fixed hourly rate that the Contractor may charge for professional services performed in support of the Telematic Asset Tracking Services.

Contractor – A Vendor that enters a Term Contract with the Department as a result of this solicitation. The Contractor is responsible for the system and all services and related equipment whether directly performed or through a third-party provider.

Customer – A State agency or Eligible User.

Customer Data – All data collected, generated, received, maintained, processed, inferred, or stored through the solution in connection with a Customer, including raw device data, location and trip data, driver and vehicle information, diagnostic and maintenance data, alerts, reports, configurations, audit logs, metadata, attachments, and derived data.

Department – The Department of Management Services, a State agency.

Eligible User – As defined in Rule 60A-1.001, F.A.C.

Fleet Management Information System - The State of Florida's Fleet Management Information System ("FMIS"). The State's FMIS is the official repository of all records regarding the effective and efficient use, operation, maintenance, repair, and replacement of the State's fleet. FleetWave is the current FMIS utilized by the State.

Geofencing – The creation of a configurable virtual boundary around a physical location using GPS, Wi-Fi, cellular networks, Radio Frequency Identification (RFID), or other wireless technologies, through which entry, exit, presence, or dwell events may trigger alerts or automated actions.

Global Positioning System (GPS) – A satellite-based navigation network that provides continuous, worldwide positioning, navigation, and timing information.

Hardware – GPS trackers, sensors, gateways, or vehicle-installed devices and other related equipment as needed by the Customer. May be used interchangeably with "device(s)." The requirements and deliverables set forth in this Scope of Work related to Hardware are only applicable if Hardware is offered as a part of the Contractors solution.

Manufacturer – The company who manufactures and directly sells Telematic Asset Tracking Services and Related Equipment. Manufacturers are allowed to submit a Proposal to this RFP. Resellers are not permitted to submit a Proposal.

Non-On-Board Diagnostic (Non-OBD): A telematics or asset-tracking device or solution that does not use a vehicle's standardized OBD-II diagnostic interface to obtain power or access diagnostic and operational data. Instead, it relies on alternative power sources and communication interfaces, such as hardwired electrical connections, vehicle data buses, or internal batteries to provide location tracking and other telematics functions.

Non-Original Equipment Manufacturer (Non-OEM) – A new, unused telematic Hardware intended for the Asset, manufactured by an entity other than the vehicle or equipment manufacturer and installed after manufacture. Also known as aftermarket telematics Hardware.

On-Board Diagnostics II (OBD-II) – A standardized diagnostic interface on vehicles that can also serve as a connection point for GPS tracking and telematics devices.

Original Equipment Manufacturer (OEM) – Telematics technology, embedded Hardware, data, or services provided or authorized by the Manufacturer of the vehicle or equipment.

Order – An agreement between the Customer and Contractor which establishes the services agreed upon by the Customer and Contractor and may be used interchangeably with “purchase order” or “customer order.”

Recovery Point Objective – The maximum tolerable amount of data loss measured in time.

Recovery Time Objective – The maximum tolerable amount of time the system can be down before causing major harm to the business.

Role-based Access Control (RBAC) – The clear, distinct separation of user roles, duties, and permissions within a RBAC system.

Security Incident – An actual or reasonably suspected event that jeopardizes, or may jeopardize, the confidentiality, integrity, or availability of the solution, Customer Data, an Asset, a device, or a Customer information technology resource, including unauthorized access, malware, ransomware, data loss, service compromise, or a material violation of security requirements.

Services – Installation, configuration, support, maintenance, and training.

Software as a Service (SaaS) Telematics Solution – A software delivery model in which the provider hosts, operates, maintains, secures, and updates the solution, and authorized users access it through the internet, typically through a subscription. For this solicitation, the SaaS solution may include Asset tracking, Geofencing, dashboards and analytics, reporting, user management, API access, mobile applications, and other telematics capabilities.

State – The State of Florida.

Sub-processor – A third party that stores, transmits, accesses, processes, secures, supports, or otherwise handles Customer Data on behalf of the Contractor.

Telematic Asset Tracking Services and Related Equipment – Includes, but not limited to services that collect, transmit, and present location and operational data for physical Assets through a centralized software platform. These services monitor, manage, and report/track on the location, movement, status, and utilization of vehicles, maintenance, fuel consumption, equipment, trailers, containers, and other mobile or fixed Assets in real-time or closest industry standard. Reference to “Telematic Asset Tracking Services and Related Equipment” includes any related equipment which is needed to provide Telematic Asset Tracking Services and may be used interchangeably with “solution,” “system,” or “application.”

Term Contract – The legally enforceable State Term Contract, as defined in section 287.012, F.S., between the Department and the Contractor.

Turnkey Telematics Solution - A fully managed, end-to-end Telematic Asset Tracking Service in which the Contractor furnishes and is solely accountable for all components including but not limited to, telematics device(s), connectivity, installation, the hosted software platform, data delivery, training, and support.

Value-Added Services - Includes any additional services the Contractor offers, for no additional cost to the Customer, as part of the Term Contract, and which clearly exceed the minimum requirements and are within the scope of this Term Contract. Any Value-Added Service proposed by the Contractor, if accepted by the Customer, shall become a requirement and be a part of the minimum requirements contained in any resulting purchase order.

3 SCOPE OF WORK

3.1 Description of Scope

Contractors shall provide Telematic Asset Tracking Services and Related Equipment in accordance with the scope contained herein. During the 2026 Legislative Session, proviso language in the General Appropriations ACT (GAA) directed the Department of Management Services to competitively procure Telematic Asset Tracking Services for use by state agencies through a state term contract. The services must include, at a minimum, real-time automated tracking, monitoring, and reporting of vehicle usage, maintenance, location, and fuel consumption. Each participating vendor must agree to provide data in accordance with a unified standard established by the Department.

The Telematic Asset Tracking Services and Related Equipment solution may be delivered as a Turnkey Telematics Solution or a Software as a Service (SaaS) Telematics Solution as defined in this Scope of Work, or a combination of both solutions. Regardless of the delivery model proposed, the Contractor shall ensure the solution meets all requirements set forth in this Scope of Work.

The Hardware related requirements and deliverables set forth in this Scope of Work apply only to Contractors that propose Hardware as part of their proposed solution.

Telematic Asset Tracking Services and Related Equipment will be provided on an as-needed basis with no guaranteed or minimum spend. The Customer-Specific Scope of Work ("CSOW" or "Customer SOW") will be determined and agreed upon by the Customer and the selected Contractor as set forth in the Customer Order.

3.2 Contractor Requirements

The Contractor shall provide all Telematic Asset Tracking Services and Related Equipment required by the Term Contract and each Order. The Contractor is the prime contractor and remains responsible for all deliverables, warranties, security obligations, service levels, Sub-processors, carriers, installers, Manufacturers, and other third parties used to perform the Contract. The Contractor shall have the ability and provide the following:

3.2.1 Installation and Warranty

Requirements:

- Installers shall be trained and authorized for the applicable Hardware and related equipment and vehicle or equipment type.
- All Hardware shall have a warranty of three (3) years from the date of acceptance by the Customer.
- The Hardware warranty shall include repair or replacement of defective Hardware at no additional cost to the Customer.
- The Hardware and related equipment, components, and installation must not void the vehicle or equipment warranty.

Deliverables:

- Install and configure required equipment at multiple locations throughout the State of Florida in accordance with the Customer SOW.
- Contractor shall maintain installation and configuration records for each Asset.
- Complete Customer acceptance testing for each installation or deployment. Acceptance testing shall include testing the successful installation, device communication, data accuracy, user access, required reporting, federated identity, Application Programming Interface (API) access, and integration testing, as applicable. Billing shall not begin before Customer acceptance.

3.2.2 Hardware and Related Equipment

Requirements:

- All in-vehicle Hardware and related equipment should withstand the environmental and operating conditions of the applicable Asset, including vibration, temperature, dust, tampering, water, salt, and brine.
- Ability to detect when the Hardware or related equipment is not functioning normally (including possible device tampering detection) and generate an alert.
- The Hardware shall store sufficient data to preserve at least seven (7) consecutive days of normal Asset operation at the contracted sampling and event-capture settings. Upon restoration of connectivity, the device shall automatically transmit stored data in chronological order without loss or duplication.
- Provide integration with Original Equipment Manufacturer (OEM) and aftermarket telematics devices based on the list of OEM partners as provided in Attachment M, Technical Proposal Response.
- Access to a supply of Hardware and related equipment that meets the demand for Customers and ongoing replacement statewide within 30 days of contract award.
- Provide a Hardware option for Non-On-Board Diagnostic (OBD) vehicles and equipment.
- Provide a Hardware and related equipment options for vehicles with auxiliary equipment (e.g., plow-up and plow-down controls, emergency lighting, sirens). For vehicles outfitted with specific alarms, the Global Positioning System (GPS) vehicle-mounted device must be able to alert the specified individual(s) or groups when a vehicle alarm event is triggered.
- The Hardware shall:
 - Use unique device credentials and secure configurations;
 - Prohibit shared default credentials;
 - Protect administrative interfaces;
 - Support authenticated, digitally signed firmware; and
 - Maintain a complete inventory of device model, serial number, firmware version, carrier, support status, and assigned Asset.
- Operate in read-only mode on vehicle networks by default. Any write, command, ignition, immobilization, or vehicle-control capability requires explicit Customer authorization and documented safety and cybersecurity controls.
- Provide at least twenty-four (24) months' advance notice of reasonably foreseeable Hardware, firmware, carrier, or network end of support events.
- Replace or migrate devices rendered unusable by Contractor-selected technology or carrier changes without imposing unanticipated charges on Customers.

3.2.3 Design, Configuration, and Functionality

Requirements:

- Present information in a consistent, intuitive, and easy to use manner with:
 - Simple screen layouts and navigation;
 - Customer requested dashboards;
 - Consistent placement of commonly used functions; and
 - Data, menus, icons, and actions required to navigate the interface should not require instruction to a user with basic office computer skills.
- The solution shall allow authorized users to configure GPS and telematics data collection settings for each vehicle without requiring physical access to the installed GPS device.
- User interface must be interactive and able to pan, zoom in and out, fit all, zoom to a selected vehicle, zoom to address location, etc.
- User interface must be accessible from Customer's internal network and from off-site.
- Display location information on supported mobile devices (e.g., iPhone, Android, etc.).
- Provide the hosted solution and APIs continuously, 24 hours per day, 365 days per year, in accordance with the availability and maintenance requirements in this Scope of Work.
- Support the then-current and immediately preceding major versions of Google Chrome, Microsoft Edge, Mozilla Firefox, and Apple Safari, unless a Customer-approved exception applies.
- Provide Customer-managed Role-based Access Control (RBAC), least-privilege permissions, separation of duties, organizational hierarchies, and restrictions by Customer, business unit, fleet, Asset, function, and data type.
- Provide a hosted telematics solution, including Hardware and related equipment options, connectivity, back-end systems, reporting, administration, security, backup, recovery, and business continuity.
- The ability to integrate data with the State of Florida's third-party applications or other GPS systems through published web services or APIs.
- The user interface shall support management of GPS and telematics data, reports, analytics, Assets, vehicles, users, roles, organizational groups, and authorized local-account recovery. It shall include search and reporting tools, data and presentation export capabilities, scorecards, dashboards, and driver-behavior analysis.
- Segregate each Customer's data, users, configurations, reports, and administrative functions from those of other Customers while supporting Customer-defined organizational hierarchies and expressly authorized Department-level reporting.
- Meet applicable federal and State accessibility requirements.

Deliverables:

- Provide a current Voluntary Product Accessibility Template (VPAT) or equivalent accessibility conformance report upon request by the Customer or Department.
- Include a comprehensive help solution (including user friendly/frequently asked questions and error messages) to the Customer and Department.

3.2.4 Information Security and Privacy

Requirements:

- The Contractor and solution shall meet all applicable requirements of the following:
 - 282.318, F.S.;
 - Chapter 60GG-2, F.A.C., State of Florida Cybersecurity Standards;
 - Chapter 60GG-4, F.A.C., Cloud Computing; and
 - National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0.
 - These requirements apply to hosted environments, Hardware, firmware, mobile applications, APIs, connectivity, and Sub-processors used to provide the Services.
- All Customer Data will be encrypted in transit and at rest using current, industry-accepted cryptography and maintain documented key-management, certificate-management, and credential-rotation practices.
- Provide least-privilege access, separation of duties, privileged-access controls, secure remote access, session controls, and logging of authentication, authorization, data export, configuration change, API, support, and privileged-administrator activity.
- Perform background screening appropriate to the sensitivity of access for Contractor and Sub-processor personnel who can access nonpublic Customer Data, production environments, cryptographic material, or privileged functions.
- Notify the affected Customer and the Department of an actual or reasonably suspected Security Incident as soon as possible, but no later than four (4) hours after discovery. Initial notification shall not be delayed pending completion of an investigation.
- Following notification of a Security Incident, the Contractor shall:
 - Preserve evidence;
 - Provide available indicators of compromise;
 - Support containment, forensic analysis, notifications, and recovery activities;
 - Provide continuing status updates; and
 - Submit a root-cause and corrective-action report within ten (10) Business Days after containment unless otherwise approved by the Customer or Department.

Deliverables:

- Upon request, provide an annual System and Organization Controls (SOC) 2 Type II report or equivalent independent security assessment appropriate to the solution and Customer Data. The Contractor shall promptly provide remediation status for material findings.
- Upon request, provide security logs and relevant event data to the Customer or its designated security platform in a documented, machine-readable format without additional charge.

3.2.5 Identity and Access Management

Requirements:

- Support federated single sign-on using OpenID Connect (OIDC) and Security Assertion Markup Language (SAML) 2.0.

- Customers shall be able to authenticate users through their own identity provider (e.g., Microsoft Entra ID, Okta, or an equivalent service) without establishing separate vendor-managed passwords.
- Support Customer-enforced multifactor authentication (MFA), just-in-time (JIT) provisioning, automated user provisioning and deprovisioning through System for Cross-domain Identity Management (SCIM) 2.0 or an equivalent documented interface, and mapping of identity-provider groups to Customer-defined roles and permissions.
- Permit vendor-managed local accounts only when authorized by the Customer. Local, emergency, and service accounts shall use MFA where technically feasible (or other compensating controls when not), unique credentials, defined owners, expiration or periodic review, and complete audit logging.
- Prohibit shared, generic, and default accounts. Customers shall be able to immediately revoke access, manage roles, restrict privileged functions, and review active users and entitlements.

3.2.6 Cloud Hosting, Data Residency, and Business Continuity

Requirements:

- Store and process all Customer Data, including backups, replicas, disaster-recovery copies, system logs, and metadata, within the continental United States.
- Prohibit Contractor and Sub-processor personnel from remotely accessing nonpublic Customer Data from outside the continental United States without prior written approval from the affected Customer and the Department. Identify all hosting, backup, support, and disaster-recovery locations.
- Maintain geographically separate, redundant infrastructure, protected backups, a documented disaster recovery plan, and regularly tested recovery procedures sufficient to meet the availability requirements of this Scope of Work, including a Recovery Time Objective (RTO) of four (4) hours and a Recovery Point Objective (RPO) of fifteen (15) minutes for hosted Customer Data, unless a Customer Order establishes more stringent requirements.

Deliverables:

- Contractor shall provide a disaster recovery plan to the Department prior to contract execution and to the Customer upon request.
- Notify the Department and affected Customers of material changes to the disaster recovery plan, hosting regions, backup design, or shared infrastructure.

3.2.7 Data Ownership, Permitted Use, Access, Retention, and Portability

Requirements:

- Customer Data is and remains the exclusive property of the applicable Customer or the Department. The Contractor receives no ownership interest of Customer Data and may use Customer Data solely to perform the Contract.
- The Contractor and its Sub-processors shall not sell, disclose, monetize, commercially exploit, advertise against, combine with unrelated Customer Data, or use Customer Data to train or improve an artificial intelligence or machine-learning model without express, written authorization from the affected Customer and the Department. These restrictions apply to identifiable, aggregated, and de-identified Customer Data.

- Support Customer-configurable retention, applicable public-records and records-retention requirements, legal holds, preservation of original values and audit history, and timely production of electronic records with associated metadata.
- Do not delete Customer Data except at the Customer's written direction or under an approved retention configuration. Upon authorized deletion, permanently delete applicable production copies and provide a written destruction certificate. Protected backup copies shall expire through the documented backup cycle.
- Strictly segregate Customer Data. Department or cross-Customer access shall be limited to contract administration, expressly authorized statewide reporting, or other access approved by the affected Customer.

Deliverables:

- Provide a written certificate of destruction following authorized deletion of Customer Data.
- Provide each Customer continuous access to all its current and historical Customer Data, including raw and derived data, reports, configurations, Geofences, roles, audit records, maintenance history, attachments, and metadata.
- Provide self-service and requested bulk export in open, nonproprietary, machine-readable formats, including CSV and JSON, at any time and at no additional charge. Do not impose data-egress, API, extraction, archival-retrieval, or reasonable-volume charges.

3.2.8 API Access, Interoperability, and Unified Data Standard

Requirements:

- Provide documented RESTful APIs using OpenAPI 3.x or a successor standard, OAuth 2.0 authorization, and secure machine-to-machine service accounts or client credentials.
- Provide transactional, bulk, and incremental access to Assets, vehicles, devices, drivers, locations, trips, Geofences, diagnostics, fuel, maintenance, alerts, users, groups, configurations, and audit records.
- Provide configurable webhooks or equivalent event-based delivery for priority events, alerts, device status, and data changes.
- Maintain API availability of at least 99.9 percent per calendar month.
- Provide at least twelve (12) months' advance written notice before implementing a breaking API change or retiring an API. During the notice period, the Contractor shall maintain backward compatibility to allow Customers sufficient time to update their integrations.
- Provide complete API documentation, data dictionaries, sample code or requests, a nonproduction test environment, API activity and error logs, published rate limits, and technical integration support.
- Provide APIs, credentials, reasonable usage, standard integrations, webhooks, and data transmission without additional license, per-call, transaction, or data-egress charges.
- When authorized by the Department, the Contractor shall provide standardized data feeds, connections, or data exports to integrate the solution with the State of Florida Fleet Management Information System (FMIS). The Contractor shall support integration for both the Department and each Customer using industry-standard interfaces and nonproprietary data form.

3.2.9 Service Levels, Monitoring, and Performance

Requirements:

- Maintain hosted solution and API availability of at least 99.9 percent per calendar month, measured separately. Scheduled maintenance is excluded only when performed outside normal Customer operating hours, announced at least five (5) Business Days in advance, and limited to four (4) hours per month.
- Provide 24-hour notice of emergency maintenance when reasonably possible and notice as soon as practicable in all other cases. Emergency maintenance exclusions shall not be used to avoid chronic performance obligations.
- Provide support through documented severity levels and escalation procedures.
 - **Priority 1 incidents (Critical)** receive support 24 hours per day, 365 days per year, with an initial live response within 30 minutes and continuous work until service is restored or an acceptable workaround is implemented.
 - A Critical incident that causes a complete or significant loss of service, severely impacts business operations, or presents a safety or security risk (e.g., complete outage of telematics solution, GPS devices stop reporting location data statewide, APIs are unavailable, preventing critical integrations, Customers cannot access the system, Security Incident requiring immediate response, etc.).
 - **Priority 2 incidents (High)** initial response within two (2) hours.
 - A High or significant degradation of service affecting one or more Customers or a major business function. The system remains operational, but important functionality is impaired (e.g., Mapping or dashboard functionality unavailable for a Customer, Geofence alerts not being generated, reports cannot be generated, large number of devices offline within a region, API performance is significantly degraded but still operations, etc.). A temporary workaround may exist.
 - **Priority 3 incidents (Medium/Normal)** initial response within one (1) Business Day.
 - A non-critical issue that has minimal operational impact or involves a routine request (e.g., user account or permission issue, dashboard configuration assistance, incorrect report formatting, minor mapping display issue, general technical assistance, minor software defect with little operational impact, etc.). The system remains functional, and a reasonable workaround is available.
- Notify the Department and affected Customers promptly of a service level failure and provide a root-cause and corrective-action report for a material or recurring failure.

Deliverables:

- Measure and report monthly availability, API availability, latency, device connectivity, data completeness, data accuracy, duplicates, errors, Security Incidents, support response, recovery performance, and scheduled and unscheduled outages to the Customer or Department.

3.2.10 Transition and Exit Assistance

Deliverables:

- Within ninety (90) calendar days after Term Contract execution, provide the Department a documented exit and transition plan addressing data extraction, configuration export, Customer notification, migration, read-only access, responsibilities, dependencies, timing, security, deletion, and costs.
- Upon expiration or termination of the Term Contract or an Order, provide complete Customer Data and documentation in the required open formats at no additional charge and continue secure read-only access for up to one hundred eighty (180) days at the Customer's request.
- Provide a final complete Customer Data export within ten (10) Business Days after request and reasonable migration assistance at the Contracted Professional-Service Rate, if applicable. The Contractor shall not withhold Customer Data because of a billing or contract dispute.
- After the Customer confirms successful transfer and authorizes deletion, remove Customer Data from active systems within thirty (30) days and from backups through the documented backup cycle, not to exceed ninety (90) days, and provide a written destruction certificate.

3.2.11 Real-time Automated Tracking and Location

Requirements:

- Provide continuous, automated, real-time tracking or closest industry standard of each Asset's position, movement, and status, and reliable historical tracking data.
- Automatically determine each Asset's position using Global Navigation Satellite System (GNSS) or equivalent technology.
- Provide horizontal location accuracy of ten (10) feet or better for at least ninety-five percent (95%) of readings under open-sky conditions when adequate GNSS signal is available. The solution shall report an accuracy or confidence indicator when available and disclose environmental or technical limitations.
- Transmit data over commercial wireless connectivity (e.g., cellular and/or satellite).
- Display each Asset on a live map with current status (e.g., moving, idling, stopped, ignition on/off) and provide a trip history that includes the detailed route (breadcrumb trail).
- Highlight a vehicle or Customer group location on a map.
- Provide a user interface map to display Asset items with the ability to filter by defined group or vehicle classes.
- The ability to customize the display of specific information that is applicable to individual users (i.e., the Customer does not need to see the information for another Customer).
- Support Geofencing with multiple configurable zones, entry/exit/dwell alerts, established by the Department or Customer by driver or vehicle, with management of landmarks/points of interest.
- Determine if vehicles are active (currently in service and available for assignment or use) or inactive (temporarily or permanently out of service, retired, disposed of or otherwise unavailable for use).
- Resolve the direction of a vehicle (i.e., what direction a vehicle was traveling).
- Verify VIN and plate information for all vehicles.

- Reference officially recognized and existing street names within the State of Florida.
- Enable the Department or Customer to determine the last location of a vehicle in an accident related claim or incident for a specified time period.
- Alerts on crashes or abnormal activity.
- Support enhanced protection for law-enforcement, investigative, executive-protection, emergency-response, and other sensitive Assets, including restricted roles, masked identifiers, limited historical access, optional delayed map display, enhanced audit logging, and exclusion from statewide or cross-Customer dashboards unless expressly authorized.
- Incorporate optimal route functionality between multiple points, including accepting information from other systems indicating obstructions, traffic, etc., either through a third-party plug-in or natively within the solution.
- Identify or accept one (or many) trip event(s) for a vehicle, where a trip is defined as an origin, waypoints, and destination.
- Capture event timestamps in Coordinated Universal Time using ISO 8601, preserve the source-device timestamp, display the applicable local time zone, and capture odometer or mileage values sufficient to support trip, mileage, utilization, and audit reporting.
- Provide configurable event and exception alerts (e.g., speed thresholds, unauthorized/after-hours movement, Geofence events) via email and in-platform notification.
- Under normal GNSS and commercial wireless conditions, make at least ninety-five percent (95%) of location and priority event data available in the user interface and API within sixty (60) seconds of the source-device timestamp. The Contractor shall report latency and disclose excluded conditions.
- At a minimum, transmitted data shall include stable Customer, Asset, vehicle, device, driver, and trip identifiers; source-device and platform timestamps; location and accuracy; speed and heading; ignition and movement status; odometer and engine hours; available OBD-II diagnostic data; fuel and idling data; Geofence and rule events; alerts; device health; data source; units of measure; and data-quality indicators.

3.2.12 Vehicle Usage, Maintenance and Monitoring

Requirements:

- The ability to establish Geofences (geographic work areas) by the Department or Customer, and by driver or vehicle.
- The capability to uniquely identify the driver.
- Automatically capture per-Asset utilization including distance/mileage, engine run time, idle time, trip start and stop, and days and hours of use, etc.
- Provide standard and ad hoc usage reports at the Asset, agency, and location levels that are exportable in common formats to the Customer or Department, upon request.
- Support utilization analysis to flag under- and over-utilized Assets to inform reassignment and right-sizing.
- Support association of usage with an assigned operator.
- Capture driver behavior and safety events (e.g., speeding, harsh acceleration, braking, cornering, seatbelt status, etc.).
- Actively monitor and analyze enterprise alert trends to identify Geofencing alerts, systemic risk, control weaknesses, and noncompliance.

- Flag the Department and Customers with reoccurring, aging, or unresolved alerts and formally escalate when required.
- Ability to capture and transmit diagnostic codes from all existing and future manufacturer code listings that conform to all OBD and OBD-II standards.
- Ability for the Department or Customer to report and analyze engine operating hours.

3.2.13 Fuel Consumption

Requirements:

- Monitor fuel level and usage, fuel economy, and fuel-related events.
- Report fuel efficiency (e.g., miles per gallon or equivalent).
- Provide fuel and idling reports as requested by the Department and Customer.

3.2.14 Notification and Reporting

Requirements:

- Ability to provide Customers or the Department with unified data including, but not limited to: Assets installed, planned installations, device and connectivity status, latency, and data-quality metrics such as completeness, accuracy, timeliness, duplicate rates, and error rates.
- The ability to pull real-time or closest industry standard engine Diagnostic Trouble Codes (DTCs), engine vehicles installed, installations planned, and data quality metrics (e.g., completeness, accuracy, and error rates).
- The ability to pull real-time or closest industry standard engine DTCs, engine and vehicle health, odometer-based and engine-hour-based service scheduling, battery/voltage, and maintenance alerts.
- Provide preventive-maintenance scheduling and reminders by mileage, engine hours, and/or elapsed time, with alerts for upcoming and overdue service.
- Maintain per-Asset maintenance history (e.g., events, dates, mileage and engine hours at service) and produce reports supporting lifecycle and replacement decisions.
- Enable the Customer to configure the solution for custom notifications (e.g. e-mail, pop-up, audible, phone call, etc.) to multiple Department users, Fleet Managers and drivers, and to receive telematic information on vehicles as it occurs or in designated intervals (e.g., engine fault codes, total idle time, engine hours, fuel consumption).
- Enable the user to perform a structured search by defining values for fields that may include: date created, created by, vehicle information, etc.
- The ability to create an online digital form for manual vehicle / equipment inspections.
- The capability to support different configuration options while also having the capability of consolidating the data for a centralized Fleet enterprise view.
- Ability to provide custom reporting capabilities to include custom reports and forms that can be developed for use within the system and be updated.
- Provide APIs for the system which allows for generation of custom reports created and maintained by the Customer or Department.
- Customized and ad hoc reports as requested by the Customer or Department.
- The capability to export data from the system in a format specified by the Department that is compatible with and can be uploaded into the State of Florida FMIS.

3.2.15 Training and Technical Support

Requirements:

- Training shall include system administration, end-user operation, device installation, software functionality, and reporting capabilities.
- Technical support shall include help desk services, troubleshooting assistance, remote diagnostics where available, software and firmware updates, warranty support, and clearly defined escalation procedures.
- Ongoing support shall be available throughout the Contract term to ensure the reliable operation of the telematics asset tracking solution.

Deliverables:

- Provide comprehensive training and technical support for all telematics Hardware, software, and associated services to the Customer or the Department.
- Provide user documentation, installation guides, and online training resources to the Customer or the Department.

3.3 Customer-Specific Scope of Work

Customers shall use the Request of Quotes in accordance with Section 3.9 of this Scope of Work. For any purchases off this Term Contract, Customers may develop a Customer-Specific Scope of Work (SOW) which establishes tasks, deliverables, and specific requirements for the requested Telematic Asset Tracking Services and Related Equipment. The Customers may include the Customer-Specific SOW in the Request for Quotes issued to the awarded Contractor(s), and the Customer-Specific SOW may be incorporated into any purchase order or contract issued by the Customer. Customers are permitted to request terms and conditions which supplement those contained in the Term Contract but shall not conflict with the terms of this Term Contract. The Customer may also include additional financial consequences beyond those stated in Section 3.12 of this Scope of Work. The Customer-Specific SOW may include, but is not limited to the following:

- Statement of purpose
- Customer-specific required deliverables and tasks
- Customer-specific criteria for completion related to deliverables and tasks
- Contractor responsibilities including but not limited to: reporting requirements, data export and integration, data quality, dashboards and analytics, historical data retention
- Disaster recovery plan
- Customer-specific financial consequences for non-performance
- Customer-specific terms and conditions
- Customer-specific payment terms

Customer Data is and remains the exclusive property of the applicable Customer or the Department. The Contractor receives no ownership interest in Customer Data and shall comply with the data ownership, permitted-use, access, portability, retention, and deletion requirements of this Scope of Work.

3.4 Pricing

Attachment C, Cost Proposal shall include the Contractors Total Cost of Proposed Solution Per Asset (Total Cost) for the initial and renewal terms of the Contract. The Customer and Contractor may negotiate a lower Total Cost in the Customer's SOW. The Total Cost shall include all services, fees, related equipment, and other costs necessary to provide the proposed solution.

The Total Cost submitted by the Contractor shall be in compliance with all federal, state, and local labor laws.

3.5 Price Adjustments

The Contractor shall provide initial and renewal term Total Cost as provided to the Department in Attachment C, Cost Proposal. The Department will not allow for price increases throughout the life of the Contract unless specified in the renewal pricing submitted by the Contractor. Price decreases are allowable.

3.6 Add-On Services and Related Equipment (Optional)

Only Add-On Services and Related Equipment on the Attachment C, Cost Proposal may be purchased with a Telematic Asset Tracking Services and Related Equipment solution under a purchase order. Add-On Services and Related Equipment, without a corresponding price entry on the Attachment C, Cost Proposal shall be free of charge and considered a Value-Added Service if included on a resultant purchase order. Suggested, but not required, Add-On Services and Related Equipment may include but is not limited to:

- 3.6.1** Provide hazardous-road-condition information using lawfully obtained camera or third-party data and artificial intelligence. The Contractor shall disclose data sources, geographic coverage, usage rights, latency, accuracy limitations, false-positive controls, retention, human validation, and whether any Customer Data is used to train or improve a model.
- 3.6.2** Provide Customer-authorized capability, support driver identification and vehicle enablement. The solution shall use strong authentication and encryption, maintain complete command audit logs, provide documented local override and fail-safe procedures, and shall not remotely immobilize a moving vehicle.

3.7 Value-Added Services

Contractors may offer additional services which clearly exceed the minimum requirements and are within the scope of this Contract, at no additional cost to the Customer. If the Contractor proposes Value-Added Services in response to a Request for Quote and are accepted by the Customer, the Value-Added Services shall become a requirement and be a part of the minimum requirements contained in any resulting purchase order.

3.8 Compliance and Compatibility

It is the Contractor's responsibility to ensure that the Commodities and contractual services supplied are compliant with the Term Contract requirements, specifications, terms, and conditions. Additionally, the Contractor shall ensure that all Commodities and contractual services ordered by the Customer are fully compatible with each other and with any associated pre-existing Commodities and contractual services possessed by the Customer and disclosed to the Contractor by the Customer. The Contractor's acceptance of the Customer's order shall indicate that the Contractor agrees to deliver a Commodity and contractual service(s) that is fully compliant and compatible with the Customer's order requirements, specifications, terms, and conditions. The Contractor shall support Customer compliance with applicable federal and state requirements, including but not limited to, section 282.318, F.S.; Chapters 60GG-2 and 60GG-4, F.A.C.; the NIST Cybersecurity Framework 2.0; Chapter 119, F.S.; records-retention requirements; and applicable accessibility requirements. Order acceptance constitutes the Contractor's confirmation of compliance and compatibility.

3.9 Request for Quotes Requirement

Customers shall use a Request for Quotes (RFQ) in accordance with sections 287.056(2), F.S. and 287.0591(5), F.S., and Rule 60A-1.043, F.A.C., as applicable, when making purchases under this Enterprise Wide Agreement.

For purchases of contractual services and information technology (IT) commodities, the Customer shall issue an RFQ to all contractors awarded under this Contract. If more than 25 contractors are awarded under this Contract, the Customer shall issue an RFQ to at least 25 approved contractors.

For purchases of non-IT commodities where the purchase meets or exceeds Category 2, the Customer shall request at least two quotes from awarded contractors. State agencies shall document the justification for any selection based on receipt of fewer than two quotes.

For all purchases made pursuant to this Enterprise Wide Agreement, the Contractor recognizes and agrees that it is responsible for all tasks, deliverables, terms, and conditions, contained in this Enterprise Wide Agreement, any Customer RFQ, and any resulting Customer-specific contracts. The Contractor warrants that it has fully informed itself of all relevant factors affecting the accomplishment of the tasks and deliverables and agrees to be fully accountable for the performance thereof.

3.10 Punchout Catalog and Electronic Invoicing

The Contractor is encouraged to provide an MFMP punchout catalog.

The punchout catalog provides an alternative mechanism for suppliers to offer the State access to Products awarded under the Term Contract. The punchout catalog also allows for direct communication between the MFMP eProcurement System and a supplier's Enterprise Resource Planning (ERP) system, which can reflect real-time Product inventory/availability information. The punchout catalog enables Florida buyers to "punch out" to a supplier's website. Using the search tools on the supplier's Florida punchout catalog site, the user selects the desired Products. When complete, the user exits the supplier's punchout catalog site and the shopping cart (full of Products) is "brought back" to MFMP. No orders are sent to a supplier when the user exits the supplier's punchout catalog site. Instead, the chosen Products are "brought back" to MFMP as line items in a purchase order. The user can then proceed through the normal workflow steps, which may include adding, deleting, and editing Products (i.e., line items) in the purchase order. An order is not submitted to a supplier until the user approves and submits the purchase order, at which point the supplier receives an email with the order details.

The Contractor may supply electronic invoices in lieu of paper-based invoices for those transactions processed through MFMP. Electronic invoices may be submitted to the Customer through one of the mechanisms as listed below:

1) EDI (Electronic Data Interchange)

This standard establishes the data contents of the Invoice Transaction Set (EDI 810) for use within the context of an Electronic Data Interchange (EDI) environment. This transaction set can be used for invoicing via the Business Network (formerly known as Ariba Network) for catalog and non-catalog goods and services.

2) PO Flip via BN

This online process allows Contractors to submit invoices via the BN for catalog and non-catalog goods and services. Contractors are able to create an invoice directly from their

inbox in their BN account by simply "flipping" the PO into an invoice. This option does not require any special software or technical capabilities.

The Contractor warrants and represents that it is authorized and empowered to and hereby grants the State and the third-party provider of MFMP, a State contractor, the right and license to use, reproduce, transmit, distribute, and publicly display within MFMP. In addition, the Contractor warrants and represents that it is authorized and empowered to and hereby grants the State and the third-party provider the right and license to reproduce and display within MFMP the Contractor's trademarks, system marks, logos, trade dress, or other branding designation that identifies the Products made available by the Contractor under the Term Contract.

3.11 Financial Consequences

Failure to comply with the requirements of the Term Contract will result in the imposition of financial consequences. The following financial consequences will apply for the Contractor's failure to meet the performance metric standard and due date corresponding with the deliverables under the Term Contract. The Customer may impose additional Financial Consequences beyond those stated herein to apply to that Customer's purchase. The State of Florida reserves the right to withhold payment or implement other appropriate remedies, such as Term Contract termination, or nonrenewal, when the Contractor has failed to comply with the provisions of the Term Contract.

The financial consequences below will be paid and received by the Department of Management Services within 30 calendar days from the due date specified by the Department. These financial consequences below are individually assessed for failures over each target period beginning with the first full month or quarter of the Term Contract performance and every month or quarter, respectively, thereafter.

**Department of Management Services
Financial Consequences Chart**

Deliverable	Performance Metric	Performance Due Date	Financial Consequence for Non-Performance
Contractor will timely submit complete Term Contract Quarterly Sales Reports	All Term Contract Quarterly Sales Reports will be submitted timely with the required information	Completed reports are due on or before the 30 th calendar day after the close of each State fiscal quarter	\$250 per day late
Contractor will timely submit complete MFMP Transaction Fee Reports	All MFMP Transaction Fee Reports will be submitted timely with the required information	Completed reports are due on or before the 15 th calendar day after the close of each month	\$100 per day late

No favorable action will be considered when Contractor has outstanding Term Contract Quarterly Sales Reports, MFMP Transaction Fee Reports, or any other documentation owed to the Department or Customer, to include fees / monies, that are required under this Term Contract.

3.12 Customer-Specific Financial Consequences

The Customer-Specific financial consequences outlined below may be incorporated into the Customer-Specific SOW. This list is not all-inclusive, and the Customer reserves the right to require further financial consequences.

Customer-Specific financial consequences are not the Customer's exclusive remedy for non-performance. Repeated or chronic failure may result in a corrective-action plan, suspension of new Orders, nonrenewal, or termination of the Order.

**Customer
Financial Consequences Chart**

Deliverable	Performance Metric	Performance Due Date	Financial Consequence for Non-Performance
Hosted solution or API availability	At least 99.9% monthly availability, measured separately	Monthly	Five percent (5%) of affected monthly recurring charges for each 0.1 percentage point below the standard, capped at 25% per month
Priority 1 incidents (Critical) support response is 24 hours per day, 365 days per year	Initial live response within 30 minutes, with continuous work until restoration or acceptable workaround	Per incident	Two percent (2%) of affected monthly recurring charges per failure, capped at 20% per month
Recovery objectives	RTO of 4 hours and RPO of 15 minutes for hosted Customer Data	Per event	Ten percent (10%) of affected monthly recurring charges per failure
Security Incident notification	Notification within 4 hours after discovery	Per incident	\$1,000 for each hour or portion of an hour late, capped at \$25,000 per incident, in addition to other available remedies
Customer Data export and transition	Complete export within 10 Business Days and required read-only access and deletion certification	Per request or transition	\$500 per day late and reimbursement of documented incremental migration costs caused by the delay