Federal Motor Carrier Safety Administration

Attachment 2 - TruData Modernization IT Support

Statement of Objectives
11/14/2025

TABLE OF CONTENTS

TRUDATA MODERNIZATION IT OPERATIONS SUPPORT

STATEMENT OF OBEJCTIVES (SOO)

INTRODUCTION

The Federal Motor Carrier Safety Administration (FMCSA) intends to procure services to continue the modernization of the TruData Platform using native Amazon Web Services (AWS) technologies to enable efficient data storage, exchange, and analysis for improving the registration, inspection, compliance, and enforcement (RICE) mission functions for FMCSA. This Statement of Objectives (SOO) outlines high-level outcomes expected by FMCSA and the tasks required to streamline data exchanges between mission applications and eliminate redundant capabilities delivered by other systems, such as SAFER and SAFETYNET, and other data structures implemented solely for information sharing between systems. In addition, the successful contractor will closely coordinate the Office of the Secretary of Transportation (OST) to ensure that the underlying infrastructure for the new data platform is operating at a level optimal for the health of mission applications and other analytical applications.

AGENCY MISSION

FMCSA was established within DOT on January 1, 2000, pursuant to the Motor Carrier Safety Improvement Act of 1999 (49 U.S.C. 113). Formerly a part of the Federal Highway Administration, FMCSA's primary mission is to prevent commercial motor vehicle-related fatalities and injuries. Activities of the Administration contribute to ensuring safety in motor carrier operations through strong enforcement of safety regulations; targeting high-risk carriers and commercial motor vehicle drivers; improving safety information systems and commercial motor vehicle technologies; strengthening commercial motor vehicle equipment and operating standards; and increasing safety awareness. To accomplish these activities, FMCSA works with Federal, State, and local enforcement agencies, the motor carrier industry, labor safety interest groups, and others.

FMCSA places safety as the highest Agency priority. To support this priority, FMCSA has established a strategic framework that contributes to meeting its mission of saving lives and making America's roads safer, both by providing more efficient access to safety information and developing new tools for enhancing the enforcement processes. This strategic framework is shaped by three core principles:

- Raising the bar for entry to the Commercial Motor Vehicle (CMV) carrier industry
- Maintaining high safety standards, through monitoring the CMV industry
- Removing high-risk carriers, drivers, and service providers from operation

BACKGROUND

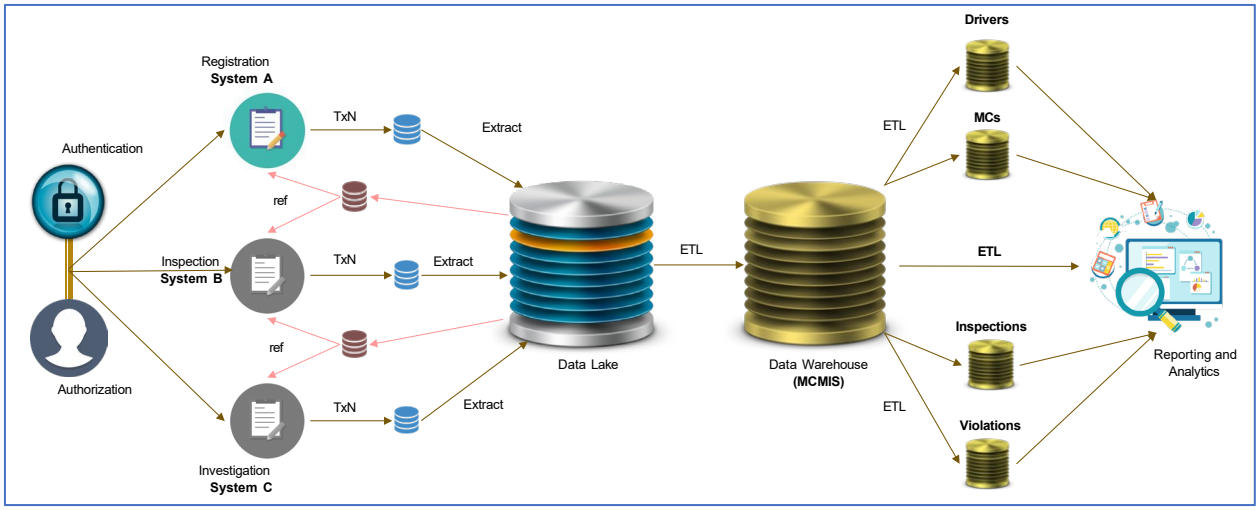
FMCSA is a data sharing organization that focuses on transportation safety through the consolidation, processing, and dissemination of motor carrier safety data. FMCSA has an on-going Business Processes and IT management effort to provide more efficient access to safety information. This program was put in place to support FMCSA's core principles and to introduce modern IT processes for supporting the FMCSA Mission Systems. The Office of the

Chief Technology Officer (MC-I) was established in 2020 to align IT services with RICE and implement modern tool and technologies to enable FMCSA's mission.

The current application portfolio includes applications built on a variety of application development platforms, contemporary and deprecated. In addition, the applications present varying degrees of maturity in terms of documentation available. The contractor will collaborate with MC-I to utilize the information available to establish a baseline and mature the state of documentation available for the data infrastructure. The IT infrastructure that supports the applications and systems has been in Amazon Web Services (AWS) virtual private cloud (VPC) since 2016 and is managed by OST up to the Operating System layer, i.e., amazon machine image (AMI) provisioning and infrastructure architecture implementation is handled by OST.

Since 2021, MC-I has engaged in establishing an authoritative data platform using AWS-native technologies to streamline data capture from various data sources and data sharing with FMCSA stakeholders, including state partners and law enforcement agencies. The implementation of the data platform is aligned with the vision, illustrated in **Figure 1**.

Figure 1. Concept of Operation for FMCSA TruData Data Platform



In its current state, the data lake is implemented using AWS S3 bucket(s) and the data warehouse and data marts are implemented using Amazon Redshift.

SCOPE

The supported work involves the application of IT project management, communication and architecture best practices, principles, and techniques to support IT efforts and initiatives. This will enable MC-I to improve, maintain, or develop a variety of systems and operations which have significant agency impact while facilitating the agency's ability to accomplish its primary mission. The IT Support services will enable FMCSA to achieve the following objectives:

Provide IT support services that will enable FMCSA to accomplish mission objectives.

Support the integration of data and capabilities from other Automated Information Systems (AISs). The data integration includes but is not limited to the data related to the document metadata and document contents.

Support a growing set of datamarts currently approaching one hundred (100).

Support the integration of data and capabilities from Automated Information Systems (AISs).

Support the current TruData AWS architecture designed and implemented in prior initiatives to support the new features as well as security, compliance, auto-scalability, monitoring and performance concerns.

Support technical concerns of data migration from the FMCSA's master systems to the TruData Platform and mitigate any availability/reliability issues.

Address applicable technical debt and plan of action and milestones (POAMs).

PERIOD OF PERFORMANCE

The base period of performance for this contract shall be for twelve (12) months with three (3) separate option periods of twelve (12) months each thereafter, for a maximum of four (4) years.

CLIN	Period	Sections
1	Base	C.1.1, C.1.2, C.1.3, C.1.4, C.1.5, C.1.6
2	Option 1	C.1.1, C.1.2, C.1.3, C.1.4, C.1.5, C.1.6
3	Option 2	C.1.1, C.1.2, C.1.3, C.1.4, C.1.5, C.1.6
4	Option 3	C.1.1, C.1.2, C.1.3, C.1.4, C.1.5, C.1.6

OBJECTIVES

The core objectives are described in detail in the following sections, and describe a user-centered, business driven, innovative approach to organizational change and capability delivery across FMSCA, including business, data, information, and technology layers.

At a minimum, this SOO supports the following goals:

The contractor shall assist with providing IT support services that will enable FMCSA to accomplish mission objectives. The scope of work covers tasks to support the FMCSA in carrying out activities to ensure effective and efficient IT management with a focus on the technical and administrative requirements for IT support services.

C.1.1 GENERAL OBJECTIVES

The Contractor shall provide an innovative technical approach to implement, support and continue the modernization of the TruData platform for FMCSA and realize the objectives outlined. Specifically:

- The Contractor shall provide non-personal, IT systems support, staffing controls, program management, and shall deliver services both on site as necessary to execute against all requirements established in this SOO and as set forth by the Government.
- All development and testing will occur within DOT/FMCSA environments, or instances of environments licensed to DOT/FMCSA, unless explicitly permitted by the COR in writing.
- Establish a development process with the entire contractor and government team that: develops end-to-end capability in an agile manner; facilitates open communication through regular check-ins and collaborative sessions; and provides clear actors/activities/documents/outcomes.

FMCSA personnel familiar with MCMIS and other legacy data sources will be available from a business/historical perspective to support the Contractor's efforts. However, the government may/may not have technical expertise with the components to explain previous software or architectural decisions made due to the age of the system. A significant amount of documentation produced during previous efforts does exist and will be available for review after contract award.

Technology Stack

The contractor shall utilize AWS native technology stack or other FMCSA provided technologies to implement, support and continue the modernization of the TruData platform for FMCSA. The technology set includes but is not limited to: Amazon Redshift, Data Pipeline, AWS Data Exchange, AWS Lake Formation, AWS Glue, Kinesis, DynamoDB, and S3.

C.1.2 OPERATIONS & MAINTENANCE (O&M)

The Contractor shall perform the following objectives:

Provide full Operations and Maintenance (O&M) support to maintain the current data platform delivering in an Agile IT environment. This will include: the day-to-day operations and maintenance support, business process documentation, requirements analysis, development of user stories, functional and technical elaboration, coding, testing production/release support, defect/bug fixes and timely administrative support.

Tasks areas under the scope of this performance work statement include:

- Task 1: Configuration Management
- Task 2: Amazon Cloud Architecture & Solutions Engineering
- Task 3: Support Services
- Task 4: Platform Support

Task 1: Configuration Management

Includes improving existing components, creating/replacing new product components, automating manual processes, and creating something new and upgrades. The specialist shall maintain a prioritized backlog within Jira of applications for assessment/audit based on the last

reviewed date. Functional Requirements, translated into Epics, Features and User Stores that will be used to populate the backlog, may include, but are not limited to:

- Continued application design and implementation
- System configuration to support business processes.
- Integration for input and output methods
- Workflow design and implementation
- Overall collaboration of applications
- Enhancement, patches, and updates to applications, data, or cloud systems
- Data import of records collected from legacy systems.

The contractor shall ensure that the data platform continues to operate in parallel with legacy MCMIS until 100% of required data elements, as specified by FMCSA, are available in the platform until legacy MCMIS is sunsetted.

Task 2: Amazon Cloud Architecture & Solutions Engineering Support Services

The contractor shall provide IT engineering and architecture support for FMCSA. The contractor shall be responsible for ensuring all work is performed as required. Once the scope is fully defined and agreed upon, the contractor shall:

(A) Continued architecture reviews using tools such as Amazon Web Services (AWS) Well Architected Framework to review architecture and make recommendations to enhance the maintainability, reliability, availability, and security of FMCSA systems.
(B) Continued support to FMCSA leadership and project teams to develop, document and implement shared services and best practices within AWS to determine technology solutions with a preference towards Cloud-Native solutions such as Azure or AWS.
(C) Continued support of IT system requirements based on business needs and perform as-needed analysis of alternatives to provide an analytical comparison of the operational effectiveness, suitability, and life-cycle cost of alternatives that satisfy established capability needs.
(D) Continued review of technical designs, code scans, security scans, test results and other development project artifacts of existing and proposed IT systems to assess solution against DOT and FMCSA design standards, mission alignment, maintainability, security, and reliability.
(E) Exercise judgment, originality, and resourcefulness in ensuring that systems and services are developed and delivered in accordance with business owner requirements and current technology.

Task 3: Support Services

Contractor shall perform the following activities in accordance with FMCSA's cybersecurity and Section 508 requirements captured in clauses, attachments and throughout the documentation.

- The Contractor shall provide technical support services for day-to-day O&M support services for FMCSA's applications and dedicated maintenance activity for legacy applications remediation or minor enhancements. This includes sustaining, stabilizing and reactive and proactive activities. Corrective Maintenance – Defect corrections – fixing errors in design and coding
- Adaptive Maintenance – Minor modifications to maintain usability in a changed environment. Threats: Modifying the software to respond to new threats; new Cybersecurity functionality. Modifying the software because of changes to policy and doctrine.
- Perfective Maintenance – Functional changes (user requests) - Modifying the functionality or adding new functionality of the software based on user requests; this includes cybersecurity functional enhancements. Performance Enhancements (no user requests) – Using more efficient coding algorithms that operate faster; functionality does not change but the operational speed does. Includes minor enhancements to existing design patterns and the existing application solution framework to keep the system viable in production to meet customer requirements.
- Preventative Maintenance: Enhance maintainability. Cleaning up the code or code optimization for better software sustainability.
- Respond to vulnerabilities remediation activities to assure that identified issues are resolved in DOT mandated timelines.

Task 4: Platform Support

The contractor shall identify applications and data sources not covered by data migration: registration, prioritize applications, data sources and use cases, and agree upon the high-level scope of Data migration: other than registration. Once the scope is agreed upon, the contractor shall:

- Support all data sources not covered under Data migration: registration.
- Maintain connectivity with all identified data sources to ingest data.
- Relate data from different data sources.
- Maintain ETL scripts for the data warehouse and data marts.
- Optimize data sharing between applications and standardize reference data for applications.
- Create/maintain reports and dashboards based on the data warehouse and data marts for data visualization and analytics.
- Provide Tier III Production support for capabilities delivered to Production.
- Support State-specific data marts to exchange safety information with states, as required by SafeSpect, PRISM and Innovative Technology Deployment (ITD) programs.
- Support the transition of data sources for Safety applications to modernized applications, when available.
- Support and maintain the current and any future datasets to the Datahub.

C.1.3 SECURITY OBJECTIVES

Ensure Department of Transportation (DOT) and FMCSA IT Security Policies and Procedures are followed during the TruData Modernization activities. The Contractor shall comply with all prevailing Department of Transportation (DOT), Federal Motor Carriers Safety Administration (FMCSA), and Federal IT Security standards, policies, and reporting requirements, which are outlined in the Cybersecurity – Privacy Requirements For Unclassified Information Technology (IT) Services. (See Appendix 1)

Provide comprehensive analysis of current applications and infrastructure that incorporates considerations for security such as data sensitivity, legal or other regulatory issues, disaster recovery, currently deployed remote access, or internal security considerations, etc. Provide technical services regarding security and privacy in the migration planning services that are consistent with the NIST Special Publication 800-144 – "Guidelines on Security and Privacy in Public Cloud Computing" or other applicable standards and guidelines.

Provide support and services in compliance and in alignment with Federal Risk and Authorization Management Program (FedRAMP) standardized security assessment, authorization, and continuous monitoring policies in migration planning services, as required by the scope of the project.

Describe framework and approach to incorporating both federal and agency security requirements into migration planning recommendations Contribute to the update of security documents detailed in the FMCSA IT Security Handbook to include system security plan (SSP), Risk Assessment Report (RAR), Security Assessment Report (SAR) and POAM documentation for the TruData Data Platform.

All documentation shall be in accordance with applicable Federal and FMCSA standards, guidance, and best practices. Vulnerability and compliance scans should be performed monthly and made available to FMCSA Cybersecurity Division for review. Scans should be conducted against operating systems, database, and web applications. Findings discovered from scans must be remediated as per FMCSA policies and procedures.

Facilitate, create, update, and deliver Security Authorization documentation associated with System Owner (SO) and Information System Security Officer (ISSO) activities for authorization/re-authorization.

Perform Risk Assessments in accordance with NIST 800-30, Rev 1. Compare and document all required TruData security implementation. Ensure that required Security Controls are identified, documented in the SSP and implemented accordingly for TruData in accordance with NIST 800-53r4.

Provide consultation on POAM or Potential Finding Remediation to assist in efficient and effective remediation of potential or actual findings in accordance with current guidance, policies, and procedures. This includes performing analysis and finding alternatives to remove or reduce vulnerabilities to a satisfactory level that meets federal, department and FMCSA security requirements. Assessment findings that need to be resolved for systems are maintained in DOC's Cyber Security Assessment Management (CSAM) tool.

C.1.4 MANAGEMENT OBJECTIVES

Maintain clear government visibility into program cost, schedule, technical performance, and risk, including periodic reporting.

Provide meaningful reporting and analytics that provide FMCSA with up-to-date and comprehensive information regarding technical and management performance.

Provide FMCSA decision making support in the form of relevant artifacts and work products.

Provide Agile Metrics and Processes to measure Agile team performance and monitor contractor's efforts, to include the collection of performance, cost and schedule data.

The contractor must fully comply with applicable statutes and demonstrate working knowledge and understanding of applicable regulations, policies, guidelines, and specifications that affect the FMCSA.

C.1.5 LABOR OBJECTIVES

The Contractor shall dedicate personnel who exhibit a professional history of implementing technical solutions and effectively communicating verbally and in writing. Due to the labor-intensive nature of this task, the Government assumes that the personnel proposed for this task will be 100% dedicated to this requirement for the life of duration of the task. FMCSA anticipates a combination of the following labor categories to perform the work under this requirement:

1. Project Manager
2. Business Analyst
3. Data Architect
4. Database Developer
5. Quality Assurance Analyst

The contractor shall propose a team based on their technical solution that shall constitute one (1) data management team working in an agile manner to support the data platform solution iteratively.

C.1.6 ADMINISTRATIVE OBJECTIVES

The Contractor shall attend a Kick-Off Meeting with the Contracting Officer (CO), Contracting Officer Representative (COR) no later than five (5) business days after the date of award. The COR will schedule the kick-off(s) meetings. Upon request and by the direction of the COR, the Contractor shall provide:

- Meeting agendas and meeting preparation material no later than two (2) hours prior to a scheduled meeting
- Capture meeting minutes and action items during the meeting
- And within one (1) business day distribute the minutes and action item list to the meeting attendees (or appropriate distribution list as agreed to and directed by the COR)

The Contractor shall be available to meet with the COR upon request to present deliverables, discuss progress, exchange information, and resolve emergent technical problems and issues.

Place of Performance

The Contractor shall perform the work both at the Contractor's facility as well as on-site at DOT Headquarters: 1200 New Jersey Ave SE, Washington, DC 20590. The contractor may be permitted to telework, as approved by the Government, to comply with the applicable guidelines or at the discretion of the COR. The Government will also provide laptop images for use on site or remote. At the Government discretion, some weekdays might be designated to be worked remotely at the Contractor's facility and/or core business hours might be established.

Hours of Operation

The core hours of operation will be between 0600 and 1800 Eastern Standard Time, Monday through Friday (except Federal Holidays). There may be occasions when Contractor employees will be required to work other than normal business hours including evenings, weekends, and holidays to fulfill requirements under this contract, which will require prior approval from the COR. The Contractor shall be available to meet and interact with FMCSA personnel during the core hours, including daily standup meetings. These meetings may be held virtually or physically or a combination of the two.

Emergency Situations

The Contractor shall provide emergency support as directed by the Government. The Contractor shall follow FMCSA emergency management and notification procedures. As directed by the CO or COR, the Contractor shall continue performance in emergency or mission essential conditions. Additionally, the Contractor may be required to account for the whereabouts of their personnel should this information be requested by the COR or CO.

Contractor Onboarding

All Contractors onboarding shall follow FMCSA security requirements. For contractors requesting a FMSCA badge, the Contractor shall provide the following information to the COR as well as the necessary onboarding forms (OF 306 & Public Trust Questionnaire).

Contractor off-Boarding

The Contractor shall notify the COR immediately of a contractor's resignation. The contractor shall notify the COR in a timely manner of any contractor leaving the contract. The Contractor shall provide the COR the contractor departing badge and Fob no later than two business days after departure.

Knowledge Transfer

As the FMCSA prepares to complete a project with the assistance of a Contractor, it desires to preserve the knowledge that the Contractor has amassed over the duration of the project. The

Government plans for a four-to-eight-week contractor transition-out phase, during which the Contractor shall provide the minimum staff to perform necessary transition for this contract.

The contractor shall collaborate and cooperate with the government and existing contractors to effectively ramp up support and execute the required services.

The contractor shall facilitate, support and conduct transition out activities as directed by the government and in cooperation with government contractors to transition-out support services inclusive of functionalities, data, and capabilities. Fully support transition-out, to include identifying, developing, and providing supporting documentation. Perform task order requirements during the transition-out process. Conduct detailed overview sessions with the new contractor as directed by the government to provide visibility and insight into the support services.

Qualifications of Contractor Personnel

The Contractor shall propose the appropriate labor mix necessary to complete each task. The Contractor shall provide trained, knowledgeable personnel according to the requirements of each task. The FMCSA will not provide or pay for training, conferences, or seminars for Contractor personnel in support, or for the performance of, their tasks, except for FMSCA-specific and specialized training not obtainable outside the FMSCA.

Employee Identification

All Contractor personnel must be recognizable as such while on any activity or work effort performed under this contract. This shall be accomplished by issuing badges and/or name tags that contain the Contractor's company name and employee's full name. The Contractor shall furnish badges or nametags for his/her employee at the Contractor's expense prior to contract performance. All employees shall wear the identification in a conspicuous place on exterior clothing. The Contractor shall ensure that Contractor personnel identify themselves as Contractors when attending meetings, answering Government telephones, providing any type of written correspondence, or working in situations where their actions could be construed as official Government acts.

To ensure the requirements of FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, are met, the Contractor shall:

- Provide a listing of personnel for whom identification (ID) card is requested to the COR or CO who will provide a copy of the listing to the card issuing office. This may include Contractor and Subcontractor personnel. Follow issuing office directions for submittal of an application package(s).
- While visiting or performing work on a DOT facility, as specified by the issuing office, CO or COR, ensure that Contractor employees prominently display their identification card.
- Promptly deliver to the issuing office: (1) all ID cards assigned to an employee who no longer requires access to the facility; and (2) all expired ID cards within five (5) days of their expiration or all cards at time of contract termination, whichever occurs first.

- Immediately report any lost or stolen ID cards to the issuing office and follow their instructions.

Non-Personnel Services

The Contractor shall provide strictly non-personnel services and shall work as an independent Contractor. Contractor employees are not subject to direct supervision and control by the Government. The Contractor shall advise and assist the Government but shall not make final decisions or certifications on behalf of the Government, nor perform any inherently governmental functions. The Contractor and its employees shall not represent the Government nor appear to represent the Government in performance of these contract services. Contractor personnel shall clearly identify themselves as Contractor employees in all interactions during contract performance.

Accessibility and 508 Compliance

All solutions and documentation shall comply with applicable 508 standards.

Accessibility Requirements (Section 508):

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public. All EIT deliverables within this BPA call shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, FMSCA identifies the following applicable EIT accessibility standards:

Section 508 Applicable EIT Accessibility Standards:
36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web- based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous JavaScript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.31 Functional Performance Criteria applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web- based Intranet and Internet Information and Applications at a minimum. Information and Communication Technology (ICT) is covered by Section 508 must confirm to the Web Content Accessibility Guidelines (WCAG) 2.0 Level A and Level AA Success Criteria and Conformance Requirements. This includes all covered web and non-web content and software.

Data Rights

The Government has unlimited rights to all documents/material produced under this contract. All documents and materials, to include the source codes of any software, produced under this contract shall be Government owned and are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. Neither contractors, subcontractors, nor anyone performing work in support of this contract shall use, sell, give, or otherwise make commercially available any documents or materials developed or provided in the performance of this contract without written permission from the Contracting Officer. All materials supplied to the Government shall be the sole property of the Government, and contractors, subcontractors, and anyone performing work under this contract may not use for any other purpose. This right does not abrogate any other Government rights.

The Government will retain unlimited rights to all intellectual property and technical data produced while developing, deploying, training, using and supporting FMCSA or other Federal agencies under this contract. All modifications to Government Off-The-Shelf (GOTS) or COTS software, middleware, hardware, or source code will be the sole property of the Government. Furthermore, the Government will retain rights to all the data contained in the systems that are in scope for this PWS, whether in electronic format or otherwise. The Contractor will be required to negotiate agreements with commercial system vendors relating to non-disclosure of vendor-proprietary information.

Except as noted above, all software and data rights developed or provided under this SOO, including any previously proprietary or commercial off the shelf software, will be provided to the Government, for any intended use by the Government. The Government will not authorize the Contractor to assert Copyright in data first produced in the performance of this contract.

Conflict of Interest

The Contractor shall provide a statement, which describes in a concise manner all relevant facts concerning any past, present, or currently planned interest (financial, contractual, organizational, or otherwise) relating to the performance of work hereunder. This statement shall include any bearing on whether the Contractor has a possible organizational conflict of interest with respect to: (1) the ability to render impartial, technically sound, and other objective assistance or advice, or (2) obtaining an unfair competitive advantage. The Contractor may also provide relevant facts that show how possible organizational conflict of interest relating to other divisions or sections of the organizations and how that structure or system would avoid or mitigate such organizational conflict.

CONSTRAINTS

Quality Assurance

The contractor shall propose a Performance Work Statement with a quality assurance surveillance plan with associated milestones required to achieve each milestone to Full Operating Capability (FOC). The Government will use a Quality Assurance Surveillance Plan (QASP) to monitor the contractor's performance.

The QASP will provide oversight help to ensure that service levels reach and maintain the required levels for performance of this task. Further, the QASP provides the Government with a

proactive way to avoid unacceptable or deficient performance. The QASP is a living document and may be updated by the Government as necessary. Any updates to the QASP must be agreed to by both the contractor and the Government.

The contractor must provide a QASP five (5) days after award. The QASP will be negotiated and discussed prior to award kick-off or shortly after. If needed, the draft QASP will be updated within ten (10) business days of contract kick off meeting by the CO, and the COR.

Contractor Access

Contractors who access FMCSA's network from outside the FMCSA's main campus have various types of access as described below:

Government Furnished Equipment (GFE)

The government may provide the following to Contractors:

- FMCSA Wi-Fi provides a no-charge access to the Internet for users who have devices with capabilities. FMCSA provides this access for Contractors that are in FMCSA buildings.
- Continuous Integration Configuration Management (CICM) Software Engineering Platform that can be accessed both internally and externally via the CICM Virtual Private Network (VPN). FMCSA and their contractors use this platform for source management, continuous integration, deployment, and release to the entire development environment.
- The government will provide the contractors with appropriate FMCSA credentials as required. GFE issuance will be tracked by machine tag number and recorded by the COR.
- The Contractor shall maintain a detailed inventory accounting system for all physical GFE/Material provided to the contractor. The inventory must specify, at a minimum: product description (make, model), Government tag number, date of receipt, name of recipient, location of receipt, and current location. The Contractor shall attach an updated inventory report to each Monthly Progress Report.

Government Furnished Information (GFI)

- Government furnished information will include system architecture diagrams, user stories (requirements), system security standards. User stories will be provided after award whereas the target system architecture diagram will be included in the SOO. Security standards will be included in the RFQ.

DELIVERABLES

The contractor shall:

- Provide deliverables as outlined in the deliverables table.
- Provide regular reporting on development in conformance with FMCSA SOO
- Ensure that the deliverables are in accordance with the contract and Task Order.
- Provide required deliverables that will be reviewed and accepted by FMCSA in accordance with the agreed upon requirements.
- Jira/Confluence is used as the official repository for all agile/project management deliverables.

Submit an invoice for each task following completion of task activities and acceptance of deliverables by FMCSA. The contractor shall also provide all data required to support the processes and procedures applicable to the tasks outlined in Section C. In addition, the contractor shall provide ad-hoc reports and respond to data calls as requested by the Government.

#	Deliverable[1]	Delivery Date(s)[2]
1	Kick-Off Meeting	Five (5) business days after contract award
2	Monthly Status Reports • Status of data migration: Planned and Completed activities. • Contract Personnel Roster, including GFE inventory for contractor personnel. • Labor hours expended	Monthly, NLT 7th day of the following month to the COR.
3	Meeting agendas, minutes, action items, risks and issues	Posted to the Project's Confluence Page
4	Problem Notification Reports, Issues, Risks and Mitigation Strategies	Verbal: During normal work hours of that day or at the beginning of the next FMCSA workday. Written: Within 24 hours after the identification of the problem.
5	Jira Backlog	At the end of each sprint, prior to the next sprint
6	Support for Post Deployment Support	As agreed upon in the final approved Contractor's Project Plan
7	Release Plan and Notes	At the end of each Release

[11] All deliverables shall be submitted electronically to the CO, and the COR in a format that is compatible with Microsoft Office 2003 / Microsoft Project 2003 (or new versions) and are subject to government review and acceptance.

[2] If a delivery date falls on a federal holiday, it shall be due the following business day.

APPENDICES

CYBER	Appendix 1 – FMCSA IT Security and Privacy Language	FMCSA IT Security and Privacy Language