



Appendix B
Table of Contents

1.0 INTRODUCTION.....4

1.1 SCOPE..... 4

2.0 FUNCTIONAL REQUIREMENTS5

3.0 TECHNICAL REQUIREMENTS6

3.1 USER INTERFACE REQUIREMENTS 6

3.2 HOSTING 7

3.3 SECURITY 7

 3.3.1 *General Requirements*..... 7

3.4 ACCESS SECURITY 9

3.5 SYSTEM SECURITY..... 10

3.6 SECURITY LOG/AUDITS/REPORTS 11

3.7 BACKUP/RECOVER/FAIL-OVER 11

 3.5 *System Management*..... 12

3.6 PERFORMANCE 13

 3.6.1 *Response Time*..... 13

 3.6.2 *System & Transaction Volumes*..... 13

3.7 INTERFACES..... 14

 3.7.1 *Interface General Requirements* 14

 3.7.2 *List of licensed accounts*..... 15

 3.7.3 *Interfaces to a Data Warehouse* 15

4.0 PROJECT MANAGEMENT REQUIREMENTS.....16

4.1 WORKING WITH STATE GOVERNANCE..... 16

4.2 PROJECT MANAGEMENT DELIVERABLES 16

4.3 PROJECT START-UP 16

 4.3.1 *Project Kickoff* 16

 4.3.2 *Project Start-up Tasks* 17

4.4 PROJECT MANAGEMENT REQUIREMENTS..... 17

 4.4.1 *Project Management Plan* 18

 4.4.2 *Scope & Change Management*..... 18

 4.4.3 *Schedule Management* 18

 4.4.4 *Quality Management* 19

 4.4.5 *Resource Management* 19

 4.4.6 *Communications & Stakeholder Management* 19

 4.4.7 *Risk & Issue Management*..... 19

 4.4.8 *Status Reporting*..... 20

4.5 DOCUMENT REPOSITORY 20

4.6 PROJECT MANAGEMENT TOOLS 21

4.7 FREQUENCY AND EVOLUTION OF PROJECT MANAGEMENT ACTIVITIES..... 21

5.0 DELIVERY22

5.1 SDLC START-UP ACTIVITIES 22

 5.1.1 *Vendor's SDLC Methodology*..... 22

 5.1.2 *System Implementation Plan/High-Level Roadmap*..... 22

 5.1.3 *SDLC Documentation and Version Control Tools*..... 22

5.1.4	Architecture & System Environments.....	23
5.1.5	Requirements Traceability Matrix.....	24
5.1.6	Capacity Analysis Plan.....	24
5.1.7	Tool and Approach Validation.....	24
5.2	INITIAL USE CASE ANALYSIS AND GAP ANALYSIS	24
5.2.1	Business Use Cases.....	25
5.2.2	Gap Analysis.....	25
5.2.3	Demonstration Environment.....	25
5.3	RELEASE PLANNING	25
5.3.1	Release Management Plan	25
5.3.2	Iterative SDLC for Each Release or Sub-Release	26
5.4	ITERATIVE REQUIREMENTS ANALYSIS AND DESIGN ACTIVITIES	26
5.5	ITERATIVE DEVELOPMENT ACTIVITIES	27
5.6	TESTING REQUIREMENTS	27
5.6.1	Vendor Testing Deliverables.....	27
5.6.2	Required Testing Activities	27
5.6.3	Test Conducted by Vendor	28
5.6.4	UAT Test Requirements.....	29
5.6.5	Testing Environments.....	30
5.6.6	Defect Management	30
5.6.7	Use Automated Testing Tools	30
5.7	DATA CONVERSION AND MIGRATION	31
5.7.1	Current Data Stores & Architecture	31
5.7.2	Document Management.....	32
5.7.3	State Data Preparation Activities.....	32
5.7.4	Legacy System Change.....	32
5.7.5	Data Conversion, Migration and Synchronization Specifications.....	32
5.7.6	Tools and Procedures	32
5.7.7	Data Synchronization	33
5.7.8	Data Quality.....	33
5.7.9	Conversion Testing	33
5.7.10	Location and Governing Policies	34
5.8	IMPLEMENTATION ACTIVITIES	34
5.9	VENDOR LOGISTICS.....	35
6.0	TRAINING REQUIREMENTS.....	36
6.1	TRAINING DELIVERABLES.....	36
6.2	TRAINING REQUIREMENTS	36
6.2.1	Required Training Activities.....	36
6.2.2	Training Plan Requirements.....	37
6.2.3	Training Material Requirements	37
6.2.4	Required Training.....	37
6.2.5	Knowledge Transfer Requirements	38
6.3	ORGANIZATIONAL CHANGE SUPPORT	38
6.4	TRAINING POPULATION	38
7.0	OPERATIONS & MAINTENANCE.....	39
7.1	GENERAL REQUIREMENTS	39
7.1.1	Scope of Operations & Maintenance (O&M) Support.....	39
7.1.2	Support Levels	39
7.1.3	Issue Resolution.....	40
7.1.4	Reporting and Management of Support Incidents.....	40
7.1.5	State Best Practices and ITIL Compliance.....	40



- 7.2 WARRANTY PERIOD 40
- 7.3 O&M SUPPORT REQUIREMENTS..... 41
 - 7.3.1 *Planning Requirements* 41
 - 7.3.2 *Support Preparation Requirements*..... 41
 - 7.3.3 *O&M Services* 42
 - 7.3.4 *Release Management Requirements* 43
 - 7.3.5 *O&M Staffing Requirements* 44
- 7.4 EXCEPTIONS, LIQUIDATED DAMAGES, BONDING, AND SLAS 44
 - 7.4.1 *Liquidated Damages* 44
 - 7.4.2 *Bonding Requirements* 46
 - 7.4.3 *Service Level Agreements (SLAs)* 46

1.0 Introduction

1.1 Scope

The State of Delaware, Delaware Department of Transportation (“DeIDOT”) through the Division of Motor Vehicles (“DMV”) currently manages the collection, auditing, reporting, and enforcement of taxes on motor fuels with its custom-built solution, FuelTracer. DeIDOT desires to implement a Commercial Off-The-Shelf (COTS) Motor Fuel Tax system to modernize its current tax administration processes. This initiative aims to enhance the efficiency, accuracy, and transparency of motor fuel tax collection, licensing, auditing, and compliance activities. By adopting a proven COTS system, DeIDOT intends to leverage industry best practices, reduce operational risks, and ensure scalability to meet future legislative and technological demands. The Motor Fuel Tax system will support electronic filing, real-time data analysis, automated workflows, and improved taxpayer services. The software employed in the system shall comply with all of the requirements described herein.

For purposes of this document, the term “DeIDOT Team” refers collectively to staff from the Delaware Department of Transportation (DeIDOT), the Division of Motor Vehicles (DMV), and the Department of Technology and Information (DTI) assigned to this project. The DeIDOT Team will serve as the State’s project management representatives and will be the primary point of contact for the Vendor regarding project execution, deliverables, and approvals.

2.0 Functional Requirements

The Motor Fuel Tax System’s functional requirements are contained in Appendix D – Functional Requirements. The Vendor is responsible for meeting all of the requirements contained in Appendix D. The Vendor must complete and return Appendix D as part of its proposal response or the Vendor’s proposal will be deemed non-responsive and will be disqualified.

Exceptions to DeIDOT’s Request for Proposals (“RFP”) that have been requested by the Vendor as part of the vendor’s proposal response are automatically rejected by DeIDOT. The only exceptions to the RFP will be those that have been negotiated by DeIDOT and awarded Vendor as part of a contractual agreement.

Please complete and return Appendix D – Functional Requirements.

3.0 Technical Requirements

This section details the technical requirements for the Motor Fuel Tax System. These requirements cover aspects of the Motor Fuel Tax System outside of the requirements for the specific business areas. The users of the system include all agency staff and external users, including but not limited to DMV Staff, motor fuel providers, motor fuel suppliers, Delaware State Treasurer and Finance staff, and other staff (e.g., law enforcement) as identified by DelDOT.

Any references to policies and associated links refer to the most current version. Vendors shall be responsible for reviewing, understanding, and complying with all such policies.

The Vendor must comply with the most current State of Delaware Standards and Policies. The policies may be updated at any time and supersede the information in this RFP, including all appendices and exhibits. The State of Delaware's standards and policies can be found at:

[Standards and Policies - Department of Technology & Information \(DTI\) - State of Delaware](#)

3.1 User Interface Requirements

- **Multiple Browser Support** - UI must support all major browsers, including but not limited to Edge, Chrome, Firefox, and Safari. Public-facing web applications shall be browser-independent.
- **Mobile GUI Support** - UI must provide a single responsive GUI (Graphical User Interface) that runs on mobile devices as well as desktop devices (preferable to include laptop/monitor touchscreen interactions).
- **Consistent Layout** - UI must have a consistent layout across modules, including warnings, alerts and other prompts, and must have consistent controls and buttons across modules.
- **Internal and External Users** - UI must consider the audience of users from internal (DMV and State staff) and external users (motor fuel tax customers).
- **ADA Compliant** - UI must be ADA compliant.
 - Must conform to the State of Delaware digital accessibility standards.
 - All digital content and functionality, including but not limited to websites, web applications, mobile applications, software, and electronic documents, shall conform to the Web Content Accessibility Guidelines (WCAG) 2.1 Level AA or the most current version of WCAG at the time of implementation unless a specific exemption is documented and approved. This requirement ensures that digital assets are perceivable, operable, understandable, and robust for all users, including those with disabilities.
- **Guided Design** – Must have a simple, clean design, be intuitive, and guide the user through the process.
- **Required Fields** - UI must visually identify the mandatory input fields (i.e., requiring user input).
 - UI must also consider dynamic mandatory input fields.
- **Field Masking** - UI fields must support a format mask that will enforce mandatory formatting for data entry, such as dates, SSNs, phone numbers etc.
- **Masked Passwords** - UI password fields must be masked on typing.
- **Data Validations** - UI must validate that all mandatory data fields have been completed when a user attempts to submit information.
- **Breadcrumb Navigation Displays** - UI should display breadcrumbs and allow users to move forward and back to prior screens to adjust data before submission and guide user navigation to required screens.
- **User Save Prompts** - UI must prompt the user to save data before exiting screens as needed.
- **Real-Time Error Messaging** - UI must interactively inform the user of errors based on real-time validations performed as the user enters data or as soon as the remote system check is completed.
- **Copy/Paste Support** - UI must support the ability to copy/paste data from one application GUI to another.
- **PII Security** - UI must adhere to security measures/specifications to prevent bulk PII loss.

- **Must comply with DTI standards.** [Data Classification Policy](#)
- **Tabbing Navigation** - UI should allow tabbing/typing through fields.
- **Navigation Focus** - Focus should go to the next logical field.
- **Dynamic Dropdowns** - UI should have dynamic dropdowns that can be filtered/narrowed down by typing.
- **Branding** – Complying with Delaware branding standards as defined by the State
- **Current Version of Windows** – The system shall be developed, deployed, and maintained to be compatible with the latest version of MS Windows and, as much as possible, be capable of running in the three most current versions of Windows. The system must be upgraded to newer versions of MS Windows if required by the State.
- **Multi-Lingual Support** – The system shall support the default language is English, but shall also support other language translations for Spanish, French and others as required by the State.
- **Spellchecking** – The system must have an industry-standard spelling and grammar review feature.

3.2 Hosting

The State is seeking a cloud-based solution with the following requirements:

- **SaaS** – The Vendor will bid a solution that is generally proposed as a COTS (Commercial-Off-The-Shelf) product on a hosted platform delivered as a SaaS (Software as a Service) solution.
- **FedRAMP** – The solution must be hosted on a FedRAMP-certified hosting platform.
- **Primary & Secondary Sites** – The Vendor shall provide a Primary Data Center location and a Secondary Site that runs redundantly, serving both as a fail-over and a Disaster Recovery site. This Disaster Recovery location shall be separated from the primary data center location and shall not be within sixty (60) miles of the primary location. All locations and sites must be within the Continental United States.
- **Compliance** – The hosting platform must meet State and Federal compliance requirements. State compliance requirements may be found in the State's Security Policies at this link: [Standards and Policies - Department of Technology & Information \(DTI\) - State of Delaware.](#)
- **Connectivity** – The vendor shall supply network connectivity between the Primary and Secondary sites to sufficiently keep the systems in sync and able to meet all disaster recovery and fail-over requirements. The vendor shall provide supply network connectivity between these locations and the State's network to support all requirements in this RFP sufficiently. The vendor shall ensure that the entire system has enough network and data throughput capacity to support all requirements in this RFP.
- **Storage** – The hosting solution shall include all storage and processing capacity to support all the requirements in this RFP.
- **Supporting Software Components** – The hosted solution shall include all software components and associated licenses necessary for the system to function fully and necessary to manage and maintain the system. This includes but is not limited to database software, operating systems, infrastructure management tools, rules engines, and workflow tools.

3.3 Security

3.3.1 General Requirements

The Motor Fuel Tax System shall meet all physical and logical security requirements, including those found in the [Delaware Information Security Policy](#) and as noted below:

- **Legislation & Policy** – Complying with and maintaining compliance with appropriate State and federal legislation, regulations, and policy.

- **Security Requirements** – Complying with State and Federal security requirements and safeguard requirements, including but not limited to:
 - Incident Reporting and Breach of Security Protocols.
 - Record Disposition/Destruction.
 - Security Controls/Standards.
 - Third-Party Data Security Controls/Standards.
- **Fail Secure** – Adhering to the principle of "Fail Secure" to ensure that a system in a failed state does not reveal any sensitive information or leave any access controls open for attacks.
- **Secure System Boundaries** – Monitoring and controlling communications at key internal boundaries (for example, Web servers, Application servers, and Database servers) within the Motor Fuel Tax System.
- **Secure Logs** – Not recording sensitive data in debug logs or other application logs created by custom code or COTS components unless the Motor Fuel Tax System encrypts the PII data.
- **Protect Data** – Prevent corruption or loss of data already accepted into the Motor Fuel Tax System in the event of a system failure.
- **Secure Components** – The Vendor shall not deploy any application to production that contains known security vulnerabilities.
- **Scanning** – The Motor Fuel Tax System shall be subject to DTI security and vulnerability scanning standards. The Vendor shall remediate any non-compliant results in an agreed-upon timely fashion as defined and agreed upon in the Operations and Maintenance section of this RFP.
- **Encryption** – Apply encryption to all data, both at rest (stored) and in transit.
- **Trusted Networks and Nodes** – Restrict network connections between trusted and untrusted networks by physically and/or logically isolating systems supporting the Motor Fuel Tax System from unsolicited and unauthenticated network traffic.
- **Configuration Reviews** – Review at regular intervals the network connections, documenting and confirming the business justification for the use of all services, protocols, and ports allowed, including the rationale or compensating controls implemented for those protocols considered insecure but necessary. Reviews shall be conducted at least twice annually.
- **Organized & Well-Managed Hosting** – The Vendor shall implement administrative, physical, and technical safeguards to protect State data that are no less rigorous than accepted industry practices, such as the current Control Objectives for Information and Related Technology (COBIT) framework or similar applicable industry standards for information security, and shall ensure that all such safeguards, including the manner in which State data is collected, accessed, used, stored, processed, disposed of, and disclosed comply with applicable data protection and privacy laws as well as the terms and conditions of this RFP.
- **Hardening Procedures** – Apply hardware and software hardening procedures, which may include, but are not limited to, the removal of unnecessary software, disabling or removing of unnecessary services, the removal of unnecessary usernames or logins, and the deactivation of unneeded features in the System configuration files, as recommended by the manufacturer to reduce the System's surface of vulnerability.
- **Data Isolation** – Ensure that State data is not comingled with the Vendor's other clients' data through the proper application of compartmentalization security measures.
- **AI Model Training** - Ensure that State data is not used to train Vendor AI models
- **Security for All Environments** – All Motor Fuel Tax system environments, such as the Test and Training environments, shall be subject to the same security requirements as those for the production environment.
- **Use of Production Data in a Non-Production Environment** – Precautions must be taken when copying data from a production environment to a non-production environment. A non-production environment can be but is not limited to, conversion, staging, development, or test environments. State data in non-production

environments must be stored securely and must have State approval before moving any protected production data to a non-production environment. Prior to moving production data from the State's environment to the Contractor's system, there must be a security scan. This scan must be done by the State or a State IT Department-approved third party. This scan can be done up to three months before the data is moved. If there is a third-party scan, the scan results must be provided to the State contact.

- **Data Breach Management** – In the event of a Data Breach (e.g., Unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal identifying information maintained by a person or business and causes or is reasonably believed to cause loss or injury to a customer or partner), the Motor Fuel Tax System and Vendor shall:
 - Immediately notify the State with information regarding the breach (e.g., time, customers affected, data compromised, etc.).
 - Isolate all systems used by the attacker to prevent further issues with the data or network.
 - Separate or disable the breached user accounts.
 - Assess the damage and identify and close all breach points.
 - Provide the capability to notify impacted parties in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system. Note there may be delays in notification if a law enforcement agency determines in writing that the notification may seriously impede a criminal investigation.
 - Identify and implement an approach to safely restore data.
 - Conduct penetration testing – depending on the breach, the State and vendor will determine which environments require penetration testing.
 - Update the system recovery and disaster recovery plans
 - Comply with the State's [Vulnerability Disclosure Policy](#)

3.4 Access Security

- **Single Sign-On Requirements** – The Motor Fuel Tax System shall comply with the State of STATE's standard identity management service single sign-on (SSO), which enables custom control of how internal and external users, referred to as "non-privileged" access, sign up, sign in, and manage their profiles, as part of the State's Identity and Access Management (IAM) strategy.

The SSO supports two industry-standard protocols: OpenID Connect and OAuth 2.0 (preferred). This identity management will handle password recovery. Multi-factor Authentication (MFA) is required for all non-privileged application Administrators and may be required for other users.

The Vendor shall provide single sign-on and identify management services for all "privileged" accounts. Privileged accounts refer to those accounts that perform development, maintenance, support or other functions required for the operation of the Vendor's solution.

- **Multiple Role Types** – The Motor Fuel Tax System shall accommodate access to customers and State employees with many roles, such as Administration, Licensing, State employees, customers, etc.
- **Personally Identifiable Information (PII)** – The Motor Fuel Tax System must protect the security of any user access to personally identifiable information collected pursuant to the Driver Privacy Protection Act ("DPPA").
- **Secure Customer and Partner Access and Two-Factor Authentication** – The Motor Fuel Tax System shall allow Clients to log into a Web-Based Transaction Center (see functional requirements, Web-Based Transaction Center) using a secure ID and password. As required by the State for some or all access, the system shall implement two-factor authentication. The vendor shall comply with the State's single sign-on policies and procedures. The Motor Fuel Tax System shall use Okta Single Sign-On implemented by the State.

- **Failed Login Attempt Lockout** – The Motor Fuel Tax System shall enforce a configurable limit of consecutive invalid access attempts by a user and implement appropriate protections to protect against further, possibly malicious, user authentication attempts using an appropriate mechanism (e.g., locks the account/node until released by an administrator, locks the account/node for a configurable time period, or delays the next login prompt according to a configurable delay algorithm) and support defined DMV and IT Department policy.

All requirements noted will be administered for non-privileged accounts through the State's SSO framework. Requirements noted shall be administered by the Vendor for privileged accounts.

- **Warning Banner** – The Motor Fuel Tax System shall display a configurable pre-login banner or warning (e.g., "System shall only be accessed by authorized users") prior to accessing any PII. If the Motor Fuel Tax System does not support pre-login capabilities, the Motor Fuel Tax System shall display the banner immediately following authorization.
- **Anti-Virus Compatibility** – The Motor Fuel Tax System shall ensure the operation of the Motor Fuel Tax System on workstations configured with anti-virus software per State standards.
- **Access Logging** – The Motor Fuel Tax System shall have appropriate logging parameters enabled to automatically monitor and record:
 - Authorized and failed access attempts
 - Critical information security events, as recommended by the operating system and application manufacturers
 - PCI and information security standards
 - User access activities
 - System exceptions

All requirements noted will be administered for non-privileged accounts through the State's SSO framework. Requirements noted shall be administered by the Vendor for privileged accounts.

- **Inactive User Session** – The Motor Fuel Tax System, upon detection of user inactivity, shall prevent further viewing and access to the Motor Fuel Tax System by that user/session and terminate the session or initiate a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures. (The length of inactivity shall be configurable.)
- **Password Rules and Access Configuration** – The Motor Fuel Tax System shall use Okta Single Sign-On implemented by the State which has password rules.

3.5 System Security

- **FedRAMP** – The Motor Fuel Tax System shall implement FedRAMP security standards. The solution should include compliance with CJIS security requirements and NIST 800-53.
- **Certifications** – The Vendor shall maintain security certifications for sites used to host the Motor Fuel Tax solution and provide the list of these certifications to DMV and IT Department staff.
- **System Audit** – The Vendor shall submit the Motor Fuel Tax System to a security audit (i.e., SOC2 Type II) annually, cooperate in State audits, and make past audit results available for evaluation purposes. The State of Delaware will determine the scope of the audit.
- **Regular Testing** – Establish policies and procedures to implement and maintain mechanisms for regular vulnerability testing of operating systems, applications, and network devices to identify:
 - Device or software misconfigurations
 - Missing software patches
 - Outdated software versions
 - Validate compliance with or deviations from the Vendor's security policy

- **Vulnerability Analysis** – Vendor shall evaluate all identified vulnerabilities for potential adverse effects on the system's security and integrity and remediate the vulnerability promptly or document the reason why remediation action is unnecessary or unsuitable. Vulnerability testing shall be conducted twice annually or more frequently as specified by other agency requirements and standards.

3.6 Security Log/Audits/Reports

The Motor Fuel Tax System shall follow State standards, including but not limited to:

- **Log All Necessary Activity** – Through configuration, all Motor Fuel Tax System components shall have appropriate logging parameters enabled to automatically monitor and record user access activities, authorized and failed access attempts, system exceptions, and critical information security events necessary to implement and achieve security, business operation monitoring, system performance, and other standards.
- **Log Data** – The Motor Fuel Tax System shall support event logging based on selectable event criteria and produce audit reports that include, at a minimum, the following:
 - Date and time of the event
 - Identity/log-on ID of the user associated with the event
 - Source of the event
 - Success or failure of the event
 - Type of event
 - Retaining (for a configurable retention period) the logs necessary to identify suspicious or questionable activity for investigation and documentation as to their cause and remediation
- **Protect Data Logs** – Any recording of sensitive data in debug logs or other application logs created by custom code or COTS components must be protected by encryption, like all other data.
- **Log Retention** – Retaining (for a configurable retention period) the logs necessary to identify suspicious or questionable activity for investigation and documentation as to their cause and remediation.
- **Important Log Data** – The log shall support the collection of security-related data, including the following:
 - Capture and store audit records for all security-relevant events, including all security, DBA, and system administrator accesses.
 - Capture and store audit records and transaction logs for indications of unusual activities, suspicious activities, or suspected violations.
 - Capture and store audit records and transaction logs for authorization of system-level changes based on criteria defined by DMV and IT Departments.
- **Usage and Performance Reports** – The Vendor shall provide security reports to the State in a mutually agreeable format, which shall include latency statistics, user access, user access IP address, user access history, and security logs for all State files related to the Motor Fuel Tax System.

3.7 Backup/Recover/Fail-Over

The Vendor shall develop, document, and implement a system continuity and backup/recovery strategy that addresses the requirements below. The strategy shall address and identify all aspects of the Motor Fuel Tax System relevant to creating continuity and recovery capabilities and any considerations internal or external to the Motor Fuel Tax System necessary to support or execute the recovery strategy.

- **Entire System** – The Motor Fuel Tax System shall support backup of all system data, configuration files, metadata, server images, and other artifacts as required to recover the Motor Fuel Tax System.
- **Supporting Environments** – The strategy must include recovery and fail-over for all environments, such as Development and Test. Although the RPO and RTO can be less than that of production, the parameters can be mutually agreed upon.

- **Disaster and Failure Events** – The Motor Fuel Tax System continuity and recovery strategy and plan shall include considerations for recovery from both disaster, non-disaster (e.g., hardware failure), and backup events.
- **Data Integrity** – The Motor Fuel Tax System continuity and recovery strategy shall specifically address data integrity, account for data dependencies across subsystems, and ensure data integrity when recovering from disaster or non-disaster events.
- **Consistent State** – The strategy shall implement a backup and restore solution to restore a consistent state across all system subsystems.
- **State Standards** – The Motor Fuel Tax System continuity and recovery strategy shall be consistent with the DMV and the State's Disaster Recovery Standards.
- **Operating Procedures** – The Vendor shall document all supporting procedures, including those to be followed:
 - During normal operations
 - When errors or failures are identified
 - When transitioning to another environment or facility
 - When transitioning back to the primary facility and environment
 - When testing the backup, recovery, and fail-over functions
 - Post recovery
- **SLA & Approval** – All operations regarding fail-over and recovery will comply with established service level requirements and include coordination with and approval by the State.
- **RPO & RTO** – Vendor will work with DMV and IT Departments to establish Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) with the following metrics:
 - RPO: A maximum of 15 minutes
 - RTO: Four (4) hours for read-only access for Law Enforcement users and interfaces
 - RTO: Twenty-four (24) hours for full system access by all internal DMV and State and web self-service clients
 - RTO: Forty-eight (48) hours for full system access by all users and clients, including third-party interfaces.
- **Point-In-Time Recovery** – Vendor's strategy shall support point-in-time and point-of-failure recovery.
- **Lost Data Logging** – In addition to requirements for logging, documented elsewhere in the RFP, the Vendor shall ensure that sufficient logging is done so that the State can take action to notify affected individuals of any transactions that may not be recoverable as a result of the RPO.
- **Encryption** – The Motor Fuel Tax System shall encrypt all backups using a shared key.
- **Backup Inventory** – The Motor Fuel Tax System shall retain Daily Backups based on agreed-upon business requirements.
- **Off-Site Storage** – The Vendor shall store Daily backups off-site.
- **Periodic Testing** – The Vendor shall test the fail-over, backup, and recovery processes at least semi-annually.
- **Root Cause Analysis** – The Vendor must identify the root cause of any system interruption in service and notify the Department of the root cause within a week of the system interruption.

3.5 System Management

The Motor Fuel Tax System shall include all of the administrative tools and capabilities that are needed to fully manage, monitor, and configure every aspect of the system, including but not limited to:

- **User Maintenance** – includes creating users, managing user roles, monitoring user activity, and administering all other attributes of users. This shall be integrated with appropriate authentication services, which are part of the complete system.

- **Customer Information Maintenance** – includes all administrative functions for managing customer information and business transactions.
- **System Administration** – includes all aspects of monitoring and overseeing system functions.
- **System Configuration** – includes all aspects of viewing, changing, checking, and managing the available system configuration information.

3.6 Performance

The Motor Fuel Tax System shall be sufficiently sized and appropriately configured in terms of memory, disk capacity, processors, network capacity, and other resources to meet the performance requirements specified below. The system must meet the peak loads as well as the average load information provided.

3.6.1 Response Time

The system shall meet the response time requirements from the viewpoint of the business user. The Motor Fuel Tax System shall be built and configured to support these requirements. The State will work with the Vendor to define the appropriate boundaries and limitations for measuring system response time.

User interface response times are categorized as follows. User interface actions that are long-running and result in response times that exceed 5 seconds should provide continuous feedback on the status of the response (e.g., a percent complete progress indicator)

User Interface Response Time Requirements		
Category	Response Time (t)	Examples
Same-Screen User Interactions	t < 0.1sec	Switching between tabs on the same screen; field-level validation; screen-level validation
Unique Record Retrieval	t < 2 sec	Search for a person, tax return, or record based on a unique identifier
Customer Search	t < 2 sec	Search for person record based on attributes (e.g., name)
Retrieve Customer Records	t < 2 sec	Retrieve and display full personal records (e.g., identifiers, demographics, photo)
Screen Transition	t < 1 sec	Move from one screen to another screen of a transaction
Save Customer Record or Transaction Information	t < 2 sec	Save or submit a customer transaction
Refresh Customer Web Screen	t < 2 sec	Customer submits information or links to another web page

3.6.2 System & Transaction Volumes

The Motor Fuel Tax system must support the State's current user population, data, and transaction volumes and be capable of supporting reasonable growth. The State's current system supports the following user community:

The State's current Motor Fuel Tax system contains the following record counts:

- More than 4000 Company records
- More than 3000 Licenses
- More than 100,000 tax returns
- More than 800,000 tax schedule details

- More than 17,000 refunds
- More than 60,000 payment records
- More than 100,000 receivables/assessments

Document imaging volume is approximately 15,000 existing records in OnBase.

The Vendor shall load all documents from the existing document imaging system into the Motor Fuel Tax System as necessary to support current customers and necessary research. The State will collaborate with the Vendor to identify documents that can be archived.

The following represents the current volume of system transactions. We expect the volume to increase steadily over the next decade.

Transaction	Annual Volume
License Renewal	350
Tax Returns	5000
Refunds	350

3.7 Interfaces

The Motor Fuel Tax System shall exchange data with various other computer systems, including, but not limited to, the Federal government, State Websites, DNREC, and State agencies.

3.7.1 Interface General Requirements

- The Motor Fuel Tax System shall initiate data exchanges both on specific system events and at scheduled times, including real-time.
- In general, the State will broker interfaces with existing state systems, resources, databases, etc.
- The Motor Fuel Tax system shall adapt to business necessary interfaces using widely adopted open APIs and standards. Software services shall be available/exposed with published documentation that would enable third-party developers to interface with other business applications.
- The Motor Fuel Tax System shall support existing processes that currently interface with the existing systems not targeted for replacement. To reduce the development and maintenance effort associated with these interfaces, State requires that the system use, where feasible, a standard interface facility or utility. It is the State's intent to reduce the overall number of interface programs, to streamline interface processes, and to use newer technological standards (EDI, web services) where feasible to exchange data.
- The Motor Fuel Tax system must extract and send data to external systems as mutually agreed upon.
- The Motor Fuel Tax System shall provide automated interfaces to and from other internal systems and external systems to maintain and synchronize dependent data.
- The Motor Fuel Tax System shall ensure the security of all data transmitted through an interface.
- The Motor Fuel Tax System shall include automatic validation processes with all interfaces to ensure that the number of records sent or received is consistent with the other node.
- The Motor Fuel Tax System shall provide APIs and/or business rules to all interface partners, ensuring that data sent to or sent by Motor Fuel Tax meets all validation rules.
- The State may, at its discretion, choose to interface with an existing system even when the core functionality is part of the Vendor's system (e.g., the State's Explorer system, which provides IRP and IFTA functionality, will not be replaced, but will be interfaced with).

- The Vendor shall recommend whether existing interfaces and extracts shall remain as they exist today, or potentially become display screens or reports in the Motor Fuel Tax System.
- The Vendor shall develop an Interface façade for interface and exchange processing. This façade shall allow other systems to access information without directly accessing the Motor Fuel Tax internal database. This should facilitate using the Cognos BI tool used by the State to create reports and analyze data.
- The Motor Fuel Tax System shall support encrypted and key-based integrations as part of its APIs.

3.7.2 List of licensed accounts

The following is a List of Licensed accounts that must be displayed by the system on Delaware's website via API. Licensed accounts should be updated in real-time as accounts are added, deleted, suspended, etc.

- [Motor Fuel - MFTA -Listing of Licensed Accounts - Division of Motor Vehicles](#)

3.7.3 Interfaces to a Data Warehouse

The Vendor must provide the capability to interface with the State's data repository. The State requires the capability to extract data from its data repository for reporting and analytics. The Motor Fuel Tax data must be integrated with the State's data repository to enable reporting and analytics.

4.0 Project Management Requirements

Project Management is ongoing for the duration of the contract. The primary objective of project management is to plan, manage, and control the timely and accurate completion and approval of all tasks and deliverables. The Vendor shall develop and execute the Project Management Plan and adhere to all scheduled due dates for all milestones.

4.1 Working With State Governance

- The Vendor shall comply with and provide support for the State's project management processes and collaborate with all governance teams, including the Steering Committee and Project Management Office (PMO).
- The State is open to any suggestions, improvements, and best practices that the Vendor can provide, which will help to reduce risk, improve process and deliverable quality, and support the overall success of the project. Changes to processes, tools, guidelines, and associated repositories will be made at the State's sole discretion after consideration of any Vendor-recommended changes. All changes will be submitted in writing, and all approvals or rejections will be transmitted via written documentation.

4.2 Project Management Deliverables

The Vendor will provide the following deliverables, which will follow the review and approval process.

- **Start-up** – Project Kickoff Materials and Sessions
- **Methodology Review, Tailoring and Plan** – Documented as a Project Management Plan (should cover all the basic PMBOK areas – Schedule, Scope, Risk, Issue, Quality/Deliverable Review & Approval, Resources, Procurement, Communications & Stakeholders). The Vendor may use agile, waterfall, or hybrid methodologies as agreed upon with the State.
- **Requirements Management** – Initial Requirements Traceability Matrix (RTM) and Requirements Management Reporting and Approach
- **Initial 90-Day Schedule** – milestones, deliverables, state staff participation tasks
- **Rolling 90-day schedule** – milestones, deliverables, state staff participation tasks
- **Vendor Project Organization Chart** – updated monthly
- **Establish Project Repository** – if not using the state's repository, state staff will be trained by Vendor staff, and selected state staff will have full admin access to all areas of the Repository to see detailed data and have access to run reports, etc.
- **Communication Approach** – status reporting, demonstrations, staff updates, leadership updates. The State typically requires weekly status reports. The State may adjust reporting frequency based on project activity levels.

4.3 Project Start-up

The Vendor is responsible for performing project start-up activities as described below.

4.3.1 Project Kickoff

The Vendor and the DelDOT Team shall plan and deliver multiple kickoff meetings as needed (and determined by the State Project Manager) to engage and coordinate with Vendor project management staff and other stakeholders. For the kickoff meeting, the Vendor shall:

- Present an overview of the Project Management Plan and the manner in which project activities will be executed.
- Include an agenda, WBS, High-Level Roadmap, presentation, and all other materials needed to detail the approach and preliminary activities for project implementation.

- Obtain approval 5 days in advance from the State for the meeting materials and agenda.
- Deliver kickoff presentation materials within 30 days of the contract execution date.

4.3.2 Project Start-up Tasks

The Master Project Schedule shall include fully detailed Contract and project start-up activities and activities for the first six months of the project, per the Master Project Schedule requirements, which shall include an overview of the timelines and phases/activities for the entire project. The following tasks shall be included in the Project Start-up tasks within the Master Project Schedule and executed:

Vendor Onboarding and Logistics

The Vendor shall, at a minimum, go through the State's onboarding Process, which includes:

- Undergo and satisfactorily pass the necessary federal and State background checks;
- Have their PCs checked for compliance with encryption and anti-virus standards by the State's IT Department;
- Receive identification badges;
- Sign non-disclosure forms and other forms as required by the State;
- Participate, as necessary, in the documentation and tracking of any equipment used throughout the project according to State and/or IT Department requirements.

Since the Vendor's staff will onboard and offboard at different times during the project, the Vendor shall designate a resource to coordinate these onboarding processes with the State. The vendor's Project Manager will review every 30 days or whenever a known change is made to ensure the appropriate people have the appropriate access to the State's equipment and data. All terminations will be reported to the State's PM immediately.

Proposed Delivery Methodology

The Vendor must use a proven project management delivery methodology. The Vendor must review and tailor the methodology with the State Project Manager to achieve the agreed-upon approach and timelines. The State will approve the proven methodology.

Contract Review

The Vendor and the DelDOT Team schedule meetings to review the awarded contract with the State team and the Vendor team so that participants can be fully informed about the project's scope and approach. This shall include this RFP and the Vendor's proposal, which will be part of the contract. The Vendor shall schedule this review within 14 days after contract execution.

Initial Project Management Plan

The Vendor shall prepare and deliver an initial Project Management Plan and timeline for delivery of updates for the entire Project Management Plan. Details of the Project Management Plan requirements are identified in the sections that follow.

All Vendor project start-up tasks or deliverables listed above are due within 60 days or sooner of the contract execution date.

4.4 Project Management Requirements

The Vendor will complete all project management activities according to project standards, which may be defined by the State throughout the project. At the State's sole discretion, any requirements may be waived.

- The Vendor shall develop, maintain, and follow a State approved Project Management Plan consistent with project and PMO standards that addresses all the project management requirements in this RFP and the awarded contract.

- The Vendor shall periodically review the Project Management Plan for any updates that may need to be applied during the execution of the Contract.
- The Vendor shall document and share any assumptions made during the creation of the Project Management Plan, including any of the sub-plans.
- The Vendor shall collaborate with the State and its representatives to incorporate all best practices and approaches into the Project Management Plan and its sub-plans.
- The Vendor shall keep the Project Management Plan current to reflect the best-known information and lessons learned throughout the execution of the project to improve project execution.
- The Vendor shall develop a high-level roadmap to organize and depict the approach for managing and executing the project, including planned development/implementation milestones.

4.4.1 Project Management Plan

The Vendor shall work with the DeIDOT Team to create a consolidated set of project management plans and deliverables and maintain them during the course of the Contract.

4.4.2 Scope & Change Management

The Vendor shall develop, present for approval, and execute a plan for defining and managing project scope, including a Work Breakdown Structure (WBS) and approach for tracking progress toward completion.

- All documentation and work products, once the scope and schedule are agreed upon by the State Project Manager, shall be subject to the agreed-upon change management process.
- The Vendor shall update the WBS and Master Project Schedule that is approved by the State as part of the change management process.
- The WBS shall clearly define all project deliverables, whether they are created by the Vendor, a Subcontractor, or the State. All deliverables will be approved in writing by the State.

Any modifications to the scope, schedule, deliverables, or costs of this project must be made through a formal written Change Order (“CO”). Change Orders shall:

- Be documented in writing and signed in advance by both DeIDOT and the Vendor prior to any work being performed;
- Identify the reason for the change and the impact on project scope, schedule, resources, and costs;
- Use the labor categories, roles, and hourly/daily rates quoted in the Vendor’s cost proposal, unless otherwise agreed in writing;
- Be priced using the methodology approved in the final contract (e.g., fixed unit pricing, time-and-materials at agreed rates, or mutually agreed fixed fee); and
- Not be considered effective until DeIDOT issues written approval.

Unauthorized work performed outside of the agreed scope without an executed Change Order shall not be billable to DeIDOT.

4.4.3 Schedule Management

The Vendor shall develop, present for approval, and execute a plan for creating, maintaining, and managing the Master Project Schedule.

- All project schedules shall include Vendor and State tasks. The Vendor shall obtain input and approval on State tasks before publishing. The Vendor may not commit State resources to timelines or tasks without State participation and approval of the schedule. The Vendor shall provide a calendar month's lead time (or other mutually agreed timeframe) to ensure that the appropriate State resources are available.

- The Vendor shall use a State-defined system (e.g., Microsoft Project) to maintain all project schedules and be capable of preparing both detailed and summary schedules.
- The Vendor shall gain approval from the State before publishing modifications to the schedule baseline. If the completion date is affected, an amendment is required.
- Project schedules shall follow PMI PMBOK project management practices. Project schedules shall clearly define dependencies, resource requirements, and the critical path of tasks, and no task shall be longer than 80 hours in duration. All project schedules shall include appropriate milestones approved by the State to allow for the overall tracking of project progress.
- All task durations and review cycles shall be calculated in State working days, not calendar duration of days.
- The Vendor shall at all times develop and propose project schedules that it believes are realistic and properly manage risk. Schedule delays that are not mutually agreed to as being caused by the State will not be considered for a change order nor additional compensation or consideration to the Vendor.

4.4.4 Quality Management

The Vendor shall develop, present for approval, and execute an approach for Quality Management. The Quality Management Plan must define the processes, oversight, and resources that will ensure that high-quality deliverables are being developed, reviewed, and presented to the State in a consistent and managed approach.

- **Project Performance Improvement** – Over the course of the project and not less than at the end of each project phase, the Vendor will fully participate in a review of lessons learned and project improvements that can be implemented.
- **Availability & Storage** – Documents, deliverables, and work products shall be stored in the agreed-upon repository and shall be viewable by the State and its agents.

4.4.5 Resource Management

The Vendor shall develop, present for approval, and execute an approach for the management of its resources on the project. The plan shall include:

- Project organizational structure
- Role and responsibility assignments, including percent of time allocated to assignments
- Staffing plan describing when and how staff will be brought onto and transitioned off the project team, retention, and where they will be located
- Background checks
- Training needs
- Details on required support from the State staff, which will help the State to allocate the appropriate resources in alignment with the project plan

Substitution of Key Personnel during the Contract term shall be approved by the State as defined in the RFP.

4.4.6 Communications & Stakeholder Management

The Vendor shall develop, present for approval and execute an approach for communicating with stakeholders and project leadership. The Vendor shall work with the State to identify stakeholders, communication needs, communication activities and tools. The Vendor shall support and participate in presentations and information sessions with State leadership, staff, and partners as necessary to facilitate the project's success.

4.4.7 Risk & Issue Management

The Vendor shall develop, present for approval, and execute an approach for risk and issue management to ensure that potential risks are identified and addressed with both a preventative mitigation and a remediation

plan. The Vendor shall develop and actively manage a risk register and issue register that shall be updated regularly as directed by the State.

4.4.8 Status Reporting

Weekly Status Meetings

- The Vendor shall meet with the State team at least weekly or less frequently as determined by the State to report status. During these meetings, the Vendor will conduct a project review (e.g., resources, schedule, issues, risks, procurement).
- The State will set the agenda and facilitate these meetings or may delegate these responsibilities to the Vendor.

Bi-Weekly Status Reports

The Vendor's Project Manager shall submit status reports to the State once every two weeks on a day mutually agreed upon by the State and Vendor. The proposed format and level of detail for the status reports will be subject to the State's approval. The report shall include, at a minimum, the following:

- Accomplishments over the reporting period
- Risk status for new or previously identified risks to any aspect of the project
- Issue status for new or previously identified issues to any aspect of the project
- Key activities over the next period
- Schedule for the next period's activities, including deliverables and dates
- Deliverables expected to finish in the next period
- Deliverables expected to start in the next period
- Identification and justification of any proposed adjustments in the schedule (time), resources (staff), scope of work, costs, or other aspects of the Project Management Plan
- Identification of schedule delays and recommended corrective action plans
- Performance reporting, including variance analysis, trend analysis, and change requests

Monthly Executive Status Meetings

On a monthly basis, the Vendor shall meet with the State's management team to report status.

- The Vendor shall provide an executive-level project review (e.g., resources, schedule, issues, risks, procurement) highlighting items that require executive attention.
- The State will set the agenda and conduct these meetings or may delegate these responsibilities to the Vendor.
- One or more meetings may be necessary to update both State staff, including DMV, IT, and other department leadership.

Quarterly Management Meetings

Every quarter or as otherwise mutually agreed, the Vendor shall present a project status report to the State staff and managers to communicate the project status to the broader State government community.

4.5 Document Repository

State's Project Artifact Repository

The Vendor shall implement and maintain a documentation repository. The State has chosen Microsoft Teams as the primary document repository and will furnish licenses as necessary to the Vendor for this purpose. If Microsoft Teams is used as the Document Repository, the State shall provide the hardware, operating system licenses, client access licenses, and Microsoft Teams Software and will be responsible for the backup and

recovery of the site. The State shall maintain administrator rights to the Microsoft Teams site. Changes to the Microsoft Teams site shall be managed by the State through a change request process to be developed jointly between the Vendor and the State.

Alternate Repository

The State is open to the Vendor providing and implementing a supplementary Document Repository platform that facilitates traceability with other project artifacts. Traceability shall be managed by the features of the tools and platform rather than manually. The State will maintain overall administrator rights of the site, and changes to the site shall be processed through a change management process that the Vendor develops with input and approval by the State. The design of the repository shall be developed in collaboration with the State and the Vendor shall obtain approval of the design from the State. The Vendor shall provide staff that can implement the approved changes to the site.

The State has the option to review and approve any Vendor-proposed tool(s) to track requirements, test cases, defects and traceability.

4.6 Project Management Tools

The State prefers to use the following project management tools unless justification is provided and agreed upon by the State as to how it would be beneficial to the State:

- Microsoft Azure DevOps
- Microsoft Project & Microsoft Project Server
- Microsoft Office
- Microsoft Teams
- Adobe

If the Vendor employs a document repository other than SharePoint as agreed to with the State:

- The Vendor shall be responsible for performing backups of any repository the Vendor establishes.
- The Vendor shall be responsible for performing appropriate training to the Agency for any repository the Vendor establishes.
- The Vendor will provide the State with the highest level of access to its information on the site.

4.7 Frequency and Evolution of Project Management Activities

The State will work with the Vendor to determine the most practical and effective approach to project management, which will evolve over time (collaboratively with the Vendor) to meet the needs of the project. The State expects that a project of this size and duration will evolve over time. The project management activities will be dynamic as well. The project management responsibilities described in this section represent a minimum set of required tasks and deliverables. The State will set the standards for project management reporting and tasks throughout the life of the project, and they will be compatible with industry standards. The Vendor is responsible for complying with those project management standards.

5.0 Delivery

As part of managing and delivering this project, the Vendor shall address all of the topics defined within this Appendix and as described below.

5.1 SDLC Start-up Activities

The following tasks shall be completed at the beginning of the project, defined in the project schedule, and approved by the State.

5.1.1 Vendor's SDLC Methodology

SDLC Requirements

The Vendor shall provide and implement an SDLC to structure and guide all system development activities. The SDLC shall meet the following requirements:

- It shall be proven, defined, documented, repeatable, and auditable.
- It must have been successfully used on a project of similar size, scope, and complexity.
- It should be consistent with industry-standard methodologies.
- Hybrid and Agile development cycles are acceptable methods.

Vendor's SDLC Documentation

It is the State's intention to have the Vendor propose and execute their SDLC methodology. The Vendor's SDLC documentation shall address the following:

- Description of the Vendor's overall SDLC methodology, including phases, activities, deliverables, and tools
- Deliverable descriptions and content outlines
- Proposed Deliverable Acceptance Criteria
- Linkage of deliverables (i.e., which deliverables serve as inputs and outputs to other deliverables)
- Phase exit and entrance criteria
- Deliverable delivery schedule (i.e., when deliverables are expected to be prepared when executing the SDLC)
- Description of the State's role
- Assumptions and constraints

SDLC Training

After the award, the Vendor shall work with the State to ensure that the Vendor and State staff are aware of and understand how to execute project activities according to the SDLC methodology and other applied standards.

5.1.2 System Implementation Plan/High-Level Roadmap

The Vendor shall prepare a roadmap that describes the overall process for the phases and iterations of the project. It shall describe SDLC processes, inputs and outputs, artifacts, participant roles, and other information to describe the overall development approach.

The Vendor shall propose an approach they believe is reasonable, appropriate, and cost-effective.

5.1.3 SDLC Documentation and Version Control Tools

The State's DMV currently uses the Microsoft suite of development and management tools, including Azure DevOps. If the Vendor prefers and proposes to use an alternate set of tools, then it shall explain and justify the choice in its proposal.

The Vendor shall use the tool(s) to track traceability between requirement artifacts, design artifacts, source code versions, version changes, and testing-related artifacts. The Vendor shall implement the agreed-upon tools to

track the versions of source code and all applicable configuration artifacts. The tools shall sufficiently handle branching and merging to allow for parallel development on different releases or other scopes of work. The Vendor shall define the strategy and plan for branching and merging to support the proposed development processes.

The version control tool(s) and their usage shall support retrieval of historic releases of the FuelTracer system, sufficient for them to be recreated in isolated environments, along with the supporting artifacts related to those releases.

The State has the option to review and approve any Vendor-proposed tool(s).

5.1.4 Architecture & System Environments

Documenting Architecture – The Vendor shall work with State staff to refine the architecture of the proposed solution and to implement all necessary system environments to properly support the complete life cycle of the project – this includes all hosted and on-premises components (e.g., hosting of interface files/components).

Environment Implementation and Management – As part of the implementation the Vendor shall develop for approval all relevant planning documents pertaining to the design and implementation of the system environments. The Vendor shall develop detailed procedures and tools for automating environment set-up, replication, and management. This includes promoting and moving software and configurations from one environment to another, data loads and scrubbing, and configuration propagation. Movement of such configurations may also include moving configurations in reverse, such as from production to pre-production, when creating fresh configurations for testing deployments.

Data Loading – The Vendor shall develop procedures and tools to support creating and loading non-production data for testing and training, periodically refreshing data in all environments, data masking, data migration, and data scrubbing.

Legacy Environment Connectivity – Environments shall be connected to and synchronized with legacy environments as required to support development, testing, training, and production.

Sizing – Environments shall be sized as appropriate for the intended use. The Vendor must include a plan for conducting performance and User Acceptance Testing in an environment that represents the production system.

On-Premises Platform Set-up – For any on-premises components, the Vendor shall define the resource requirements, and the State will lead the initial configuration effort, which will be limited to the operating system and network connectivity. The Vendor shall lead all other system configuration activities.

Environment Specific Tools – Each environment has specific requirements, including the tools that may be installed (such as debuggers in Production) or external service requirements as compared to stub applications for such services. The Vendor shall implement the required tools and technologies as part of the environment implementation.

Maintenance – The Vendor shall support and maintain all system environments, including database instances. The State is not providing any resources for day-to-day support/administration of the technical environments implemented as part of the vendor solution or development activities.

Environment Management – The Vendor shall facilitate environment scheduling and usage. The Vendor shall be responsible for data preparation, connectivity to external systems, data refresh, change documentation, and all other aspects of maintaining the environments used by the Vendor's resources and/or the State's resources, including testers and trainers.

Activity Tracking – The Vendor shall develop activity reports that can be run in each environment to document user activity, including:

- Time, Date, and User Location of Log-on and Log-off
- Transaction Activity by User per Session
- Status of each Transaction Conducted During a Session

Timing of Environment Set-up – For any equipment, all hardware and software purchases shall be timed as late as possible in the project to avoid purchasing equipment that will become prematurely outdated.

Specific Environments – The Vendor shall provide eight (8) separate environments to support implementation, including:

1. Development
2. Test
3. Training
4. UAT
5. Staging & Conversion
6. Production
7. Two others as necessary to support the project and operations

Each environment shall have separate database tables and be capable of independent operation that prevents one environment from impacting another. The Vendor shall establish additional environments as required to satisfy the Release Plan or as requested by the State through an approved Change Order.

5.1.5 Requirements Traceability Matrix

The Vendor shall use an automated tool to develop and maintain a Requirements Traceability Matrix (RTM) that shows the source of all requirements, defines them, and allows the project team to trace throughout the project to ensure that all requirements are defined, addressed, tested, and implemented. This RTM will be maintained and updated throughout the life of the project.

5.1.6 Capacity Analysis Plan

As part of the project start-up, the Vendor shall develop and document a plan for creating detailed infrastructure requirements to meet the sizing and performance needs of the FuelTracer System in production as well as the non-production environments. The approach shall include the creation of a Capacity Analysis that reviews and confirms the breadth, specifications, and sizing of the technical solution.

An initial Capacity Analysis Plan shall be developed for the project and revisited after every major release.

5.1.7 Tool and Approach Validation

The Vendor shall work with the State to validate technical approaches and tools upon which the project will depend. This task will vary depending on the Vendor's technical approach.

5.2 Initial Use Case Analysis and Gap Analysis

The Vendor shall work with the State to develop a set of use cases and corresponding models that will demonstrate the Vendor's understanding of the State system requirements and State operations. The resulting artifacts will focus all parties on the scope and functionality of the overall project.

In addition, the Vendor shall conduct a Gap Analysis with the State to compare the existing functionality of the proposed solution as it has been deployed or is being deployed elsewhere with the requirements of the State as documented in this RFP and by the Use Case Analysis. The Gap Analysis will address all functional areas, system architecture, information architecture, and system security planning.

The Gap Analysis information will be used to facilitate project planning discussions of the State's system functionality, implementation approach, and release planning. Artifacts developed for the Gap Analysis task will

not be used to define or constrain the final scope of the project, as other use cases are expected to be defined later in the project.

The Vendor shall recommend how this task can be tailored to best align with its approach and have maximum value.

5.2.1 Business Use Cases

The Vendor shall build Business Use Cases and other artifacts necessary to facilitate the analysis, based upon existing artifacts. These use cases are expected to build upon the process information and requirements presented in this RFP and leverage any workflows and process information collected by the State in preparation for the project.

Adapting Business Processes – The State is expecting that current business processes will be adapted to the functionality of the proposed solution in areas where the proposed solution has functionality that has been developed and proven for similar operations. The State will be the final decision-maker on business processes.

5.2.2 Gap Analysis

The Vendor shall prepare an approach for documenting observations and differences. The approach shall include, but not be limited to, describing how the degree of required change will be quantified or categorized. The approach shall describe how the analysis will be organized, how sessions will be conducted, what participation is required, and how results and conclusions will be reviewed with the State. The Vendor shall obtain approval from the State for the approach to documenting observations and differences and this approach shall be used by the Vendor consistently for all gap analyses.

The Gap Analysis shall address functional and non-functional requirements.

Legacy System Evolution – It is the State's goal to minimize changes to the current/legacy systems as the FuelTracer system is being planned and implemented, but legacy systems will continue to evolve over the procurement processes and as the project begins. The vendor shall work with the State to identify new functionality not included in this RFP that will need to be incorporated into the project.

5.2.3 Demonstration Environment

The Vendor shall prepare an appropriate environment as the Demonstration Environment to be used for Gap Analysis. The Demonstration Environment shall have sample data, documentation on sample data and available transactions, and shall be available to State staff in a limited capacity.

5.3 Release Planning

5.3.1 Release Management Plan

The Vendor shall work with the State to develop a Release Plan. The Release Plan will describe how the FuelTracer System may be divided into multiple releases and the order in which those releases will be deployed. Each release shall be described in terms of functionality, dependencies on other releases, and approach to data conversion and synchronization.

The State expects that the initial release will address architectural requirements fundamental to the overall design of the system and the other functional releases. Each release may be divided into smaller sub-releases. The purpose of the sub-release is to create a manageable unit of work for the Vendor and the State resources.

The Vendor shall implement a system development/system configuration process that is iterative and consistent with a proven methodology approved by the State for this project.

5.3.2 Iterative SDLC for Each Release or Sub-Release

The Vendor shall present, gain approval from the State, and follow a proven methodology that iteratively collaborates with the State to review and refine requirements, prototype components of the solution, refine and test those components and then prepare for deployment.

5.4 Iterative Requirements Analysis and Design Activities

The Vendor must develop, present for approval, and follow an iterative approach for reviewing all business functions and developing requirements and system designs collaboratively with the State staff. The Vendor shall recommend how this task can be tailored to best align with its approach and have maximum value.

Design Sessions With Staff – The State requires that the Vendor utilize design sessions as a complement to any approach to engage the participation of State staff throughout the project as necessary. Facilitated design sessions and interviews shall be conducted by the Vendor in order to fully understand and document the FuelTracer System's functional and technical requirements.

Complete Analysis and Design to Fully Define All Parts of the System – The Vendor shall analyze all information provided by the State, obtain additional information, and begin to collaboratively create and document the solution for the new system. This high-level solution shall guide all subsequent activities required in this RFP. The solution, as it continues to be refined, shall address all system requirements, including the integration with other systems.

Consistent Functionality – The sessions shall define a common design approach to ensure consistent implementation of functionality across the system. The State requires that business transactions conducted by State staff be executed with a consistent workflow and design.

Analysis and Design Sessions

The Vendor shall fully document the resulting requirements and designs using the appropriate design artifact templates. The Vendor shall obtain approval from the State for each resulting design artifact.

Analysis and design sessions will address the following:

- Design of each system function and transaction
- Functional/Non-Functional Scope of each system function and transaction
- User Interface Design and Standards for State and Business Partner Users
- User Interface Design and Standards for Public Web-based Customers/Users
- Transaction Logs and Audit Requirements
- Identity Management, Authentication, and Role Based Access Control
- Security Approach
- Database and Data Model
- Conceptual and Logical Information Model
- Infrastructure and foundation components (such as rules technology, workflow technology, report writers, and other applicable technology)
- Document Management
- Configurability
- Reporting and Analysis

The Vendor shall develop a complete list of topics to be covered in the requirements analysis and design sessions.

Experienced Facilitators

The Vendor shall provide experienced facilitators who understand the following:

- The vision for the new State system
- The State's requirements
- Motor vehicle/Tax operations

The facilitators are expected to work with the users to merge State requirements with the Vendor's proposed solution and develop a complete and comprehensive set of requirements and a documented design, including a user interface design that meets the State's needs.

5.5 Iterative Development Activities

The Vendor must develop, present for approval, and follow an iterative approach for developing and implementing the configuration of the system and any custom development. This approach must be integrated with the Analysis and Design Activities and be collaborative with the State's staff. The Vendor shall recommend how this task can be tailored to best align with its approach and have maximum value.

The development activities of the project will include the set-up and configuration of system components and programming. The State Subject Matter Experts (SMEs) will assist the Vendor during these activities to ensure that business requirements are understood and clear. During this project activity, the Vendor shall define and trace all requirements and business rules for the new system and ensure they are met.

Testing of Components

The Vendor shall plan, perform, and report on all activities required for Unit Testing. Additional requirements are found in the next section describing test activities.

5.6 Testing Requirements

The Vendor shall plan, prepare, document, and perform the following tests for each production release:

- Unit Testing
- System and Integration Testing
- Vulnerability/Penetration Testing
- Performance Testing (Volume and Stress)

The Vendor shall support the preparation and execution of UAT testing with the state team, including the development of user stories and associated test scripts.

5.6.1 Vendor Testing Deliverables

The Vendor must provide the following testing deliverables:

- Test Plan prior to each Release – this must be approved before testing begins
- Test Environment(s), Data and Scripts for each test
- Test Reports, including Defects and Results
- Execution of all tests
- Vulnerability Test Recommendations
- UAT Preparation and Facilitation and Documentation (Results, Defects)
- Certification that the Release is ready for Production

5.6.2 Required Testing Activities

For each testing effort, the Vendor shall:

- Use Enterprise Standard testing environments such as Development, System Test, UAT, etc.

- Use the agreed-upon Defect Tracking tool
- Document all test scripts in the Requirement Traceability Matrix or similar tool
- Identify data needed for testing. The State and the Vendor shall mask all data for testing. The Vendor must provide a mechanism to refresh data for each environment and build/test cycle
- Use ETL Tools to load data for this testing
- Use Automated Testing tools with regression testing where possible/feasible and/or Manual scripts to conduct these tests
- Include compatibility testing with legacy systems to verify co-existence requirements (ex: field length limits)
- Document the results, highlight deficiencies, and the approach and schedule for fixing the deficiencies

5.6.3 Test Conducted by Vendor

Unit Testing

The Vendor shall conduct unit testing on all components that are configured or developed. The Vendor shall develop Unit Test plans, execute the testing in an appropriate environment, and report in writing on all tests and results.

System and Integration Testing

The Vendor shall conduct system and integration tests to demonstrate the successful operation of the System. The Vendor shall demonstrate that the new solution is fully usable, functioning, processing data correctly, and working as designed.

System Test will focus on testing the entire system without integration into external systems. External systems will be represented by stub interfaces or leverage other approaches as appropriate and approved by the State.

Integration Testing shall include the approach and scripts used for System testing and incorporate those necessary to test the integration of the Vendor's System with external systems. The State has several third-party integrations with external systems.

As any module of the new system becomes ready, each shall undergo a system test cycle. The compatibility and continued reliability of existing modules shall be regression-tested when new modules are released.

The Vendor's system test responsibilities include but are not limited to:

- Functional testing, i.e., "black box" testing (the tester only knows the inputs and what the expected outcomes should be, and not how the program arrives at those outputs)
- Structural testing, i.e., "white box" testing (the tester knows what the program is supposed to do, and the tests are designed to fully exercise the internal components of the system)
- Testing of unexpected messages, transactions, and abnormal conditions
- Hardware and software fault testing that introduces faults into physical hardware and software
- Reliability testing that identifies and tests the ability to endure hazards, including vulnerability to attack and hacking
- Additional scenario/process variation testing that links together and invokes sequences of test cases.
- Manual and automated Regression testing, which is the repetitive testing of an application's major features to ensure that minor changes have not introduced new defects into the system
- Integrated testing of all system modules
- Installation testing that validates that the application will install and operate properly on the servers

System Testing shall verify the following:

- All functions and capabilities of the system
- Installation of software
- Conversion of data
- System, data, and application security
- Backup and recovery operations
- Accuracy and general performance
- Accuracy of documentation, manuals, and training materials
- Response time and overall system performance

By the end of the System Test phase, the Vendor shall demonstrate that all known defects have been fixed, consistent with the approach agreed upon.

Vulnerability Testing

The Vendor must run security scans and other necessary tests for every component prior to being deployed. The Vendor must conduct all scans and tests and confirm the approach with the State. The Vendor shall run all tests with guidance from the State staff. The Vendor shall interpret all results, review them with the State, and present recommendations to the State to address any security concerns.

Performance Testing

The Vendor must execute performance tests to demonstrate the solution meets performance requirements under expected user loads. The test will use peak volumes and test for higher-than-expected volumes and increasing activity levels.

The Vendor must lead the preparation and execution of a Performance Test plan that includes the use of system and network monitoring software, and system load simulation software. The Vendor must work with the State to develop/document the appropriate combinations of transactions and transaction levels to test the system.

The Performance Tests shall test:

- Response time
- Resource utilization
- Overall system performance
- Query expense evaluation

5.6.4 UAT Test Requirements

The Vendor must provide support to the State for User Acceptance Testing. This support includes the preparation of the testing environment, preparation of test data, management and support of testing tools and defect tracking system, and support tracking and documenting any defects or concerns.

The Vendor shall train State staff who participate in the testing effort and use the test tools. Staff training shall include usage of the System as well as usage of the testing tools and processes.

The State will lead the definition and execution of UAT which will be the final acceptance process by the State for the new system.

The Vendor must provide for automated data aging to allow testing of transactions with date sensitivity.

For User Acceptance Testing, the Vendor shall provide the following services:

- Use the Testing Environment established in the Set-up activities or create an additional environment for this testing

- Provide training to the state team on the solution and test tools
- Meet with the State UAT Team prior to UAT to review proposed cycles, test scripts, and available data
- Provide existing test scripts from system, performance, and penetration testing to the State UAT Team
- Provide access to the Requirements Traceability Matrix for the State UAT Team to add additional test scripts
- Identify data needed for testing. The State and the Vendor shall mask all data for testing
- Support UAT by refreshing databases, etc.
- Use ETL Tools to load data for this testing
- Provide the State UAT team with Release notes, identifying functions/capabilities fixed since the last cycle as well as new features/functionality introduced
- The State UAT Team will document the UAT results in the agreed-upon bug tracking tool. The State UAT Team and Vendor will classify and prioritize these bugs.
- Define a schedule for fixing the bugs and a cycle for retesting the bugs.
- The number of UAT cycles will depend on the phase, number/type of bugs found during previous UAT cycles and build process

5.6.5 Testing Environments

The Vendor shall set up separate system environments for test activities and shall be able to create additional environments as required.

The Vendor shall be responsible for the testing environment, refreshing the data, and the state of the environment for testing.

The Vendor shall create/update automated regression testing capabilities/scripts to test existing system components when new components are developed and prepared for deployment, where possible/feasible.

5.6.6 Defect Management

The Vendor must provide a defect-tracking system to track all system problems.

The Vendor must provide a mechanism for tracking expected versus actual test results, tracking all errors, problems and resolutions. The Vendor shall obtain approval from the State for all reports and tracking/reporting processes.

The Vendor and the State must work together to document the definition of defect classifications such as low, medium, high, and critical/blocking. All defects found during a test phase shall be classified. All defects classified as medium, high, or critical/blocking shall be fixed and satisfactorily tested prior to completion of the phase or entering into a new phase. The State has the final determination of which defects, of any classification, must be fixed prior to production and may include "low" defects such as spelling mistakes on public-facing screens.

5.6.7 Use Automated Testing Tools

The Vendor shall utilize automated testing tools and provide the documented processes to support the testing phases. It shall also provide the testing tools and licenses for the project. The testing tools, processes, and environments shall be documented and turned over to the State at the end of the project.

Any license or right to use the testing tools shall be transferred to the State for support of the system at the end of the contract. The Vendor shall provide training to State staff so that they may participate productively in the testing process.



5.7 Data Conversion and Migration

The Vendor shall work with State staff to plan and execute legacy data migration, conversion, and synchronization to the FuelTracer System. The State has identified multiple legacy data sources, including but not limited to:

- FuelTracer
- Document Management System OnBase
- Excel files

These data sources shall be analyzed, and all necessary sources shall be migrated to the new Motor Fuel Tax System as required to satisfy the business and technical requirements of this RFP and the State's needs.

The State requires that all active data and inactive data be converted, and the remaining non-converted data will be made accessible in a separate repository. The State will enable access to this separate repository of non-converted data. The State will work with the Vendor to define the data conversion plan and scope.

Based on the Vendor's release plan, some or all of the legacy databases shall be synchronized with the FuelTracer System to ensure concurrent operation of legacy systems and the FuelTracer System without data loss or risk of stale data being accessed or used for transaction processing or reporting.

Develop Plan – The Vendor shall develop a data migration, data conversion, and data synchronization/reconciliation plan that outlines the strategy and timing for these critical activities. The plan shall identify risks, risk mitigation, and recovery procedures in the event of a migration, conversion, or data synchronization failure.

Execute Data Migration Plan – The Vendor shall design, build and execute the legacy data migration, data conversion, and data synchronization solutions necessary to execute their proposed system deployment strategy. The solution shall address synchronization of file system content with database pointers as required to properly migrate all data sources required.

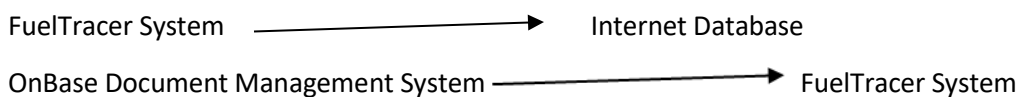
State Assistance and Collaboration – The Vendor will be assisted by the state with data mapping, identification of legacy data to be migrated, and conversion of that data from the legacy data sources to the new Motor Fuel Tax System.

Need for Flexibility – The State expects the data strategy and solution will be influenced by the architecture of the legacy applications, the architecture of the new system, and the deployment strategy.

Included in Master Schedule – Timelines for data conversion and related activities shall be specifically identified in the Vendor's Master Project Schedule.

5.7.1 Current Data Stores & Architecture

Current data store details and architecture will be provided upon project commencement; however, a high-level diagram of systems and connections is shown below. As noted above, there are multiple data stores, and the rough size of the major systems is roughly 1500 MB for FuelTracer. This data landscape will change with each major release deployment; thus, it shall be considered within the Vendor's proposed data migration, data conversion, data synchronization, and interface strategy.



5.7.2 Document Management

The Vendor and the State will collaborate to finalize the approach for document migration and storage. The approach may include the State's existing File OnBase Document Management System or a system provided by the Vendor as part of the proposed solution.

Transaction Documents – These documents are supporting documents associated with tax returns, bonds, and license application transactions, and they must be migrated into the new Motor Fuel Tax System.

The Vendor must configure the corresponding non-production environments with ECM access and prepare those environments with appropriate data.

5.7.3 State Data Preparation Activities

The State will document the current operational data for the existing system. The State is working with its legacy system staff and subject matter experts to develop documentation of the current operational data, including entity and attribute level names and definitions, constraints, validation rules, and relationships.

The State expects the results of this effort will benefit the Vendor's analysis and planning work. All results of this effort, including documentation, analyses, code, and databases, will be made available to the Vendor.

5.7.4 Legacy System Change

The data conversion and migration plan shall minimize risk to the stability of the legacy systems. The Vendor shall take appropriate actions to minimize changes to legacy systems. The Vendor shall obtain approval from the State's legacy systems staff for any proposed change that could impact the legacy systems. The Vendor shall work with the State's legacy system staff to design, develop, or deploy any required changes to legacy systems.

The data conversion and migration plan shall not require legacy system downtime exceeding the time allotted for standard system maintenance.

5.7.5 Data Conversion, Migration and Synchronization Specifications

The detailed specifications for any and all data conversion, migration, and synchronization activities will be created and approved before any of these activities are performed against production data environments. These specifications will include these details:

Source	Source Location (e.g., System/File/ Database Table)
Source Data Element	Source Data Element Identifier (e.g., SSN)
Destination	Target Location (e.g., Database Table)
Target Data Element	Target Data Element Identifier (e.g., Member ID)
Transformation/ Cleansing Rules	Describe the data transformation that is to occur, including any data cleansing.
Notes	Describe any timing constraints or anything unique about the conversion.

5.7.6 Tools and Procedures

The Vendor shall provide or develop the tools and procedures to do additional data analysis, conversion, and migration.

5.7.7 Data Synchronization

The State anticipates that a phased deployment strategy for FuelTracer Systems will require parallel operation of the legacy and new systems and that some method of data synchronization will, therefore, be required to enable continued operation of business functions not yet migrated to the new system.

Data Synchronization Solution – The Vendor shall identify, design, develop, and implement a data synchronization solution, as required, to support parallel operation of the legacy and new systems consistent with the deployment strategy. Working with State staff, the Vendor shall ensure the continued operation of business functions between legacy systems, including real-time or near real-time data synchronization if required.

5.7.8 Data Quality

The Vendor is responsible for legacy data conversion into the new system, including validating data quality and, to the extent possible, resolving data quality issues. If any data quality issues cannot be resolved, the Vendor shall document such instances and submit options for the State's consideration.

The data conversion and migration plan shall anticipate that some data records will not be convertible programmatically. The Vendor shall provide or develop any tools or user interfaces allowing State staff to manually complete or reconcile those records on a case-by-case basis. In this plan, the Vendor shall, at a minimum:

- **General Strategy** – Describe the strategy to be used to ensure data quality before and after all data conversions.
- **Data Quality Approach** – Describe the approach to data scrubbing and quality assessment of data before they are moved to the new or converted system.
- **Data Validation** – Describe the manual and/or automated controls and methods to be used to validate the conversion and to ensure that all data intended for conversion has been converted.
- **Error Detection** – Describe the process for data error detection and correction, and the process for resolving anomalies.
- **Conversion Tracking** – Audit, history, and roll-back capability for all identified data quality problems.
- **Data Quality Categorization** – Identify the types of data quality problems that may occur, including but not limited to the following considerations:
 - datatype redefinitions (e.g., alphas in dates and numbers, embedded information in codes and intelligent keys, implied content);
 - garbled content (e.g., multiple uses for a single field, freeform text values, corrupted data, un-initialized data);
 - invalid record relationships (e.g., broken chains in set relationships, orphan records (on natural key), mismatched keys (set vs. natural key));
 - invalid content (e.g., values out of defined range, code fields not on a valid list of values or lookup table, blank fields (optionality), inconsistent use of defaults);
 - context changes (e.g., import of external data, historic changes to operational parameters (system upgrades), synchronization timing of duplicated de-normalized data); and
 - behavior issues (e.g., variations in actual data from planned constraints of size, data type, validation rules, and relationships).

5.7.9 Conversion Testing

The Vendor shall ensure data conversions are validated and reviewed by the State's subject matter experts.

5.7.10 Location and Governing Policies

- **All Systems Must Be Secure** – Any system that processes or is loaded with production data must be fully secured, encrypted, and protected as if it were in production prior to accessing production data.
- **State Must Approve All Transfers** – The transfer of production data from a production system or other State data repository to any new system must have State approval before the transfer occurs.
- **DPPA** – The State and the Vendor shall comply with applicable security policies.

5.8 Implementation Activities

The Vendor shall develop and execute an Implementation Plan to ensure that all system capabilities are implemented over a rollout period and with an approach to be defined by the Vendor and the State. The State will not accept the system for consideration for production use until the successful completion of all implementation tasks is confirmed by the Vendor and the State.

Legacy System and Training Tasks – Implementation plans shall address any necessary action for the current State systems to facilitate final data conversion. The Implementation plans shall also address training and be aligned with the project's training plans.

Roll-back Plan – The Vendor shall work with the State to develop and document a roll-back plan. The roll-back plan shall identify implementation failure scenarios that could require roll-back to the legacy systems. The roll-back plan shall document the incident reporting, recovery and stabilization activities required to roll back to the legacy system, as well as the criteria for State approval to allow the Vendor to restart the implementation activities.

Implementation Requirements – As part of the implementation activities, the Vendor shall perform data conversion and migration from the legacy system to the new Motor Fuel Tax System, monitor system operations, manage and operate the new Motor Fuel Tax System, and develop or update the following:

- **Complete System** – includes all code, modules, components, and libraries kept in the production version of the data repository.
- **System Documentation** – includes all technical documentation delivered during the project (e.g., the User Guide).
- **System Performance Reports** – provides an update on system performance as the release is moved into production.
- **Implementation Notice** – formally requests approval for system changes made during the Implementation Phase.
- **Readiness Document** – consolidates summary information regarding the current status of the system and the project and provides decision-makers with the information necessary to make a "Go/No Go" decision. It shall include a checklist listing all work products, User Acceptance Test (UAT) results, other indicators of success measures, and deliverable acceptance.
- **Version Description Document** – primary configuration control document used to track and control versions of software released to the operational environment. It also summarizes features and contents for the software build and identifies and describes the version of software delivered.
- **Implementation Plan** – describes the approach, resources, and all aspects of the rollout.
- **Roll-back Plan** – describes the scenarios and failure points that will require a roll-back to the legacy systems, along with any recovery actions required to ensure data integrity.
- **Post-Implementation Review Report** – summarizes the assessment of Implementation activities at the end of the Implementation Phase.

5.9 Vendor Logistics

The State requires that certain project work, such as design sessions and project reviews, shall be performed at the State site in Dover, DE. This on-site work includes providing ongoing knowledge transfer to the State's technical staff during design sessions, status meetings, etc. The Vendor shall locate key staff positions on-site for the duration of the project when they are active on the project. Certain staff, with State approval, may be located off-site. However, the State requires the team to have frequent communication and interaction with the State staff and their on-site counterpart. The entire State-Vendor project team must be working together on coordinated tasks. If off-site work is proposed, the Vendor shall implement a team structure where all activities are represented on-site, though a portion of the activities are completed off-site.

Access to the State network and resources will be provided as necessary, per the project's needs and according to State policies.

The State will provide, as necessary:

- Workspace at the Dover, DE headquarters for on-site staff
- Work surfaces (desks)
- Network-shared printers
- File servers
- Telephones for key positions, as determined by the State
- State e-mail accounts

The State will not provide:

- Physical computer workstations (except for secure DEPARTMENT NAME workstations as necessary)

The Vendor shall provide licenses for:

- Development tools with appropriate storage and backup
- Virus Protection and Security Software for physical workstations attached to the virtual desktop infrastructure
- Other software needed for project activities

The Vendor shall provide:

- **Software** – All development and project management software and tools, with appropriate licenses for the new system's applications for all the developers' PC workstations, including the State staff. This software is expected to be installed on State hardware for State staff.
- **Peripherals** – Personal printers and other personal hardware (e.g., scanners, supplemental storage, if desired) as required at the workstation, subject to State security policy.
- **Developer Workstations** – Personal computers and displays, as required for all Vendor's staff, and sufficient to support the required development software/tools, with appropriate licenses for the operating system(s). The State will work with the Vendor to develop a workstation configuration for developers and on-site project staff. All on-site workstations will be configured and administered by the State.

6.0 Training Requirements

This section describes the Vendor training requirements.

6.1 Training Deliverables

The Vendor shall deliver the following artifacts for each production release, which shall be reviewed and approved by the State.

- **Training Needs Assessment** that identifies the number and categorization of all stakeholders who require training for their use of the system (e.g., end users, State technical support staff, etc.)
- **Training Plan** that describes each required type of training and establishes the overall plan for the components described below.
- **Training Materials** for each type of training include quick reference guides and course curriculums; training materials must be electronic, searchable, and indexed for ease of use. These materials must be reproducible and editable by the State at no additional cost. This includes, but is not limited to, computer-based training (CBT) modules, electronic documents, and printed (hard-copy) materials
- **Training/Practice Environment** and non-production data with refreshes and support for concurrent sessions, and:
 - Including a key/crosswalk that allows the ability to connect training customers to production customers
 - Data will be masked or scrambled
- **Training Schedule** for training delivery so users are educated in a ‘just in time’ approach prior to go-live.
- **Training Attendance Records** reports to show who attended each class
- **Knowledge Transfer Plan** and activities that outline the approach for transition-out activities and final training for users and technical staff

6.2 Training Requirements

6.2.1 Required Training Activities

At a minimum, the Vendor shall:

- **Develop and Update Training Materials** – Develop and maintain all training courses/curriculum, evaluations and supporting materials. Update and effectively communicate such updates to training materials and training courses, especially as defects and workarounds are identified and incremental functionality is deployed.
- **Manage & Protect Training Data** – Develop tools and mechanisms for populating and refreshing data so the information is usable for training. Where applicable, data should be masked or scrambled (e.g., FTI, PII)
- **Manage Training Environments and Data** – Establish and maintain Training and Sandbox/Practice environments with data to support training activities. These environments must be accessible in all applicable office locations.
- **Deliver Training** – Prepare and deliver the types of training listed, tracking attendance and completion.
- **Evaluate Effectiveness** – Develop metrics and mechanisms for evaluating the effectiveness of the training classes and overall training process. Implement changes as a result of the information gathered.
- **Assess Readiness** – Develop and implement a process to ensure State technical staff, including the Helpdesk and Support Groups, are prepared to support the technical operation of the solution.

6.2.2 Training Plan Requirements

The Vendor shall develop and document a Training Plan that defines and recommends a training program to ensure that all users and support staff are prepared to operate and support the system. This would include approaches for locations that cannot be closed for extended periods.

The Vendor shall provide assistance to and collaborate with the State in determining the number of classes, web-based training modules, and sessions necessary to successfully train staff.

The Training Plan shall include, at a minimum:

- **Course & Curriculum Descriptions** – Describes the list of courses and overall flow of the training, including the training materials to be used in each course and recommended hours for each course.
- **CBT and Live Training** – Inclusion of both Computer Based Training and Instructor-Led training for all users. Computer Based Training is not required for IT support staff.
- **Delivery Approach** – Delivery approach for each user type/role including Instructor-Led, Computer Based Training, webinar, etc.
- **Trainer Training** – In addition to training the entire staff on the new system, the Vendor shall also implement a Train-the-Trainer approach to prepare State training staff to onboard future State staff.

6.2.3 Training Material Requirements

The State will own and reserve the right to reproduce all training materials and content for training the varied users and to make changes to those training materials.

Training material requirements include all of the following:

- Training materials shall include, at a minimum, quick-start guides, user guides, how-to documentation, and FAQs, as appropriate.
- Training materials shall be delivered to the State to be placed in a shared location accessible to the project team and State employees.
- Training materials and courses shall describe modifications, configurations, and procedures made for the State and shall employ the State's terminology.
- Web-based courses shall be developed on standard/easily obtainable tools to allow future handoff of material for State staff to update (i.e., no custom training development toolset allowed).
- Training materials and tools shall include the capability, including licenses for any specialized tools, for State staff to update any training materials.

6.2.4 Required Training

The Vendor shall conduct the following training:

- **User Training** – Training for State staff, including Call Center/Helpdesk Staff and Authorized Agents, in advance of any production implementation to teach users how to use the completed system, including business-based scenarios.
- **Trainer Training** – Train-the-Trainer training to enable State staff to deliver training in the future
- **Test Team Training** – Tester training on all modules of the system prior to the start of each testing phase
- **Test Team Tool Training** – Tester training for State testing teams to enable them to learn the system, testing tools, processes
- **IT Staff Training** – Technical Staff Knowledge Transfer to understand solution architecture, database layouts, configuration and parameter settings, interfaces, and reporting functions. This includes ongoing sessions as well as materials to assist in transitioning.



- **Project Closeout Training** – Final round of training during Transition Out activities for any recent technical or application updates

6.2.5 Knowledge Transfer Requirements

The Vendor shall develop a Knowledge Transfer Plan that will include all activities to ensure State staff have the knowledge and skills needed to support the system.

The Vendor shall prepare a plan that describes how knowledge will be transferred throughout the project to State technical and support staff. The Knowledge Transfer Plan shall support active participation and involvement of the State’s resources from project initiation through to system turnover

Knowledge transfer to State staff shall specifically include:

- Working knowledge of the solution environment
- Working knowledge of all technical configurations associated with the System, its architecture, data file structure, interfaces, any batch programs, and any hardware or software tools utilized in the performance of this Contract
- Training on the use of system management, configuration, and development tools necessary to support and enhance the system

6.3 Organizational Change Support

As requested by the State, the Vendor shall provide assistance to and collaborate with the State in supporting the overall Organizational Change Management (OCM) effort through:

- **OCM-Related Plan Review** – Review and provide feedback on the OCM Plan
- **Content Development** – Development of additional content related to communications, training, and other implementation activities.
- **Change Analysis** – Identify differences between the current state and future state as a result of implementation.

6.4 Training Population

The following defines the population that will require training.

Category	System Scope	Count
State Staff	Entire System	50
Authorized Agents	System External Portal	100

7.0 Operations & Maintenance

The State requires a comprehensive approach by the Vendor to provide operational support for the Motor Fuel Tax System. This includes the development of support tools and methodologies that will support end users as well as provide technical support for the system. These will be implemented throughout the SDLC and for a 1-year support/warranty period once the Motor Fuel Tax System is fully operational.

The Vendor must set up and administer all hardware, software, and infrastructure components of the solution for the duration of the contract period while preparing state staff to support the solution in the future.

The Vendor must provide the operations, maintenance, support, defect management, and documentation requirements described in this section.

The Vendor must also provide a solution that meets the system recovery and performance metrics and demonstrate the solution meets these metrics during the testing of the solution.

The State may request additional support after the Warranty Period.

7.1 General Requirements

7.1.1 Scope of Operations & Maintenance (O&M) Support

The Vendor shall:

- Lead the creation of the processes and procedures related to the support of the Motor Fuel Tax System.
- Lead in the development and implementation of support tools and system support knowledge management content.
- Lead the O&M system support effort throughout the project and to the end of the warranty period.
- Work collaboratively with State support staff to ensure that they are properly prepared, trained, and have the knowledge and skills to fully lead support services after the warranty period.
- The Vendor shall provide support for all system environments as soon as they are established.
- The Vendor shall develop a training program for technical staff that will support the Motor Fuel Tax System. By the end of the warranty period, all appropriate staff, as designated by the State, shall be successfully trained by the Vendor and have the knowledge and skills for their role in supporting the Motor Fuel Tax System.
- The Vendor provides all levels of support prior to the end of the warranty period.
- Support for State computer systems is provided by the Department of Information Technology. The Vendor shall collaborate with the State, including its Department of Information Technology, to deliver support services for Project.
- The State may request additional support after the Warranty Period.

7.1.2 Support Levels

- The Vendor shall use ServiceNow as an incident and problem management ticketing system to record and track questions and inquiries until a resolution is implemented and the incident is closed. The Vendor shall propose processes and procedures for incident and problem management. The Vendor is responsible for prioritizing, categorizing, and reporting all inquiries using proposed processes and procedures. The State will collaborate with the Vendor to finalize the approach, tools, policies, and procedures. The Vendor may incorporate its own case management system into ServiceNow.
- The Vendor shall provide the initial support of the system until State staff has been trained by the Vendor to support it internally. During the course of the project, the following support model shall be used:

- **Level 1 Support** – Reception of support and operation calls shall be handled by a State-provided Help Desk. This shall include logging calls and resolving simple problems for which an existing solution has been documented or is known. Help Desk shall reference ServiceNow, the Knowledge Management System, and other tools to find documented solutions for problems. All support calls shall be logged as tickets into ServiceNow used by the State. Access will be provided to Vendor staff to ServiceNow, and it will be the Vendor’s responsibility to log tickets into their incident and problem management ticketing system if they desire so. Any call which Level 1 support cannot resolve for any reason shall be escalated to Level 2 Support. The customer will be transferred to Level 2 when the customer first calls and escalation is determined to be necessary.
- **Level 2 Support** – All Level 2 activities shall be handled by the Vendor. This includes resolution of problems and documentation of solutions. Level 2 shall be staffed with individuals capable of troubleshooting, diagnosing, and resolving a limited range of technical and system usage problems. Customer phone calls are transferred to Level 3 for immediate response only if there is an emergency. Referral to Level 3 is typically handled offline.
- **Level 3 Support** – All Level 3 activities shall be handled by the Vendor. This includes resolution of problems and documentation of solutions. Level 3 shall be staffed with individuals capable of troubleshooting, diagnosing, and resolving all technical and system usage problems either directly or by accessing related project staff.
- The Vendor shall train and confirm Level 1 staff to be prepared prior to supporting the first UAT.
- The Vendor shall train and certify State Level 2 & 3 staff during the warranty period so they are prepared to take over from the Vendor at the end of the warranty period.
- The State may request additional support from this team after the Warranty Period.
- For escalated tickets, the Vendor shall adhere to the Service Level Agreements (SLAs) described in this RFP.

7.1.3 Issue Resolution

- The Vendor shall define and implement an approach for recording, tracking, managing, and reporting on production issues and collaboratively refine it with the State and gain the State’s approval.
- The Vendor shall address all production system issues for which it is responsible within the timelines outlined in this RFP. Resolution of production system issues shall be managed through ServiceNow. The Vendor may link its case management system to ServiceNow for case management. However, all customers and State users will access issues through ServiceNow.
- The State has the option to review and approve any Vendor proposed tool(s).

7.1.4 Reporting and Management of Support Incidents

The Vendor shall track and report on incidents, including trend analysis and reporting of all application and application-related tickets.

The Vendor shall link incidents to problems and identify recurring trends.

The Vendor shall identify the root cause of all incidents and implement permanent corrective actions.

7.1.5 State Best Practices and ITIL Compliance

All aspects of the support operations, including all contributions and deliverables by the Vendor, shall be consistent with State practices and industry best practices, such as ITIL 4 standards and other standards of the State or its IT Department.

7.2 Warranty Period

- The Warranty Period for the new Motor Fuel Tax System shall start when the last release of software has been successfully moved into production, all users are migrated onto the Motor Fuel Tax System, and all

other implementation and testing activities are complete and approved by the State and the State provides written notice of System Acceptance.

- During the warranty period, the Vendor, as part of the proposed solution and services, shall:
 - Perform O&M Services, User Support and Service Desk activities, and Issue Resolution as described in this RFP.
 - Perform problem resolution and correct any identified defects in the elements of the Motor Fuel Tax System for which the Vendor had implementation responsibilities according to approved requirements. System defects covered by warranty shall include all defects preventing the Motor Fuel Tax System from performing as per the approved requirements, including but not limited to (1) all defects identified with the configuration of the Motor Fuel Tax System; (2) all defects resulting from implementation of an approved Change Request; (3) all defects resulting from customizations, custom workflows, or interfaces developed by the Vendor; (4) all defects identified in the Motor Fuel Tax System technical infrastructure and (5) issues identified with the performance of the full system or individual components of the Motor Fuel Tax System.
 - Support the production environment with the State.
 - Provide enhancements to the Motor Fuel Tax System as available time permits.
- The Warranty Period will last for one year after written notice of System Acceptance.

7.3 O&M Support Requirements

7.3.1 Planning Requirements

Staffing Needs Analysis

The Vendor shall conduct an analysis of the staffing needs for long-term support operations of the Motor Fuel Tax System based on the complexity, design, and implementation of their solution. The Vendor shall prepare formal recommendations for future ongoing State staffing to support operations.

Operations and Support Rollout Plan

The Vendor shall develop an O&M Support Rollout Plan that includes the approach, schedule, resources, and tools that shall be used to accomplish the work required in this RFP. The plan shall identify which State or Vendor staff will be trained or participate in knowledge transfer prior to UAT. The plan shall identify long term State resources who will be trained or participate in knowledge transfer prior to the end of the warranty period.

7.3.2 Support Preparation Requirements

Support Documentation

- The Vendor shall develop documentation that clearly defines the troubleshooting steps toward a solution, support processes, and problem workarounds for the Motor Fuel Tax System. Complete System Operation manuals and O&M procedures shall be developed by the Vendor; the materials shall be incorporated into training materials, reference materials, online help, other applicable materials, and the Knowledge Management System content.
- All support-related plans, outlines, drafts, final documentation and other deliverables shall be submitted to the State for approval. The documentation shall integrate with the Knowledge Management System and Standard Operating Procedure (SOP) library unless an alternate solution is presented to the State and approved by the State.

Knowledge Management System Content

- The Vendor shall work collaboratively with State staff throughout development and deployment to develop and maintain Knowledge Management System content.
- The State intends for the Knowledge Management System to be part of the proposed Incident and Problem Management Ticketing System (ServiceNow). The Knowledge Management System shall reflect that all

tickets and issues must be handled in accordance with ServiceNow procedures. The Knowledge Management System shall reflect ServiceNow processes accurately and in detail.

- The State will provide ServiceNow as the Knowledge Management System to be used. However, it is open to considering a Vendor-provided solution. Vendors proposing an existing solution that already includes a Knowledge Management System shall fully document its features in the bid response for this section.
- The State reserves the right to require the contractor to use the State-provided Knowledge Management System (ServiceNow).
- The Vendor shall work with the State and make recommendations for efficiently organizing and maintaining the Knowledge Management System content along with other support documentation and project documentation.

Help and Support Tools

- **Incident and Problem Management Ticketing System** – The Vendor shall assist the State in configuring the proposed Incident and Problem Management Ticketing System so that it properly supports the Motor Fuel Tax System’s operations.
- **Context-Sensitive Help** – The Vendor shall develop context-sensitive help as part of the proposed solution.
- **System Help Keys** – The Vendor shall implement System Help Keys as part of the proposed solution. This utility shall allow users to capture a screen when experiencing a problem and make notations for clarification on the problem, or a similar solution shall be presented. This feature shall operate within the system boundaries and the constraints established by State data loss prevention policies, which may prohibit users from printing screens or sending sensitive information via email.

7.3.3 O&M Services

- O&M services shall include both the Motor Fuel Tax System application software and the associated technical infrastructure, whether hosted or on hardware maintained by the State.
- O&M services shall be priced as a fixed-price system O&M component to cover ongoing system support from project inception through the Warranty Period.
- The State may request additional O&M Services after the Warranty Period.
- The Vendor shall provide operations support for all aspects of the Motor Fuel Tax System from inception until the end of the warranty period, in accordance with State policies and procedures.
- The Vendor shall ensure that the system operates effectively. Vendor O&M support activities shall include but are not limited to:
 - **Support Environments** – Maintain and support all Motor Fuel Tax System environments; Monitor, tune and configure the performance of the production environment as needed to comply with the Service Level Agreement (SLA).
 - **Patch and Version Management** – Patch testing and promotion to ensure all components of the State solution are operating with the latest patch levels, validated by ongoing testing, verification, and application of patches or updates provided by third-party hardware or software vendors. Vendor shall support system upgrades to the technology stack, as necessary, to maintain the latest release levels of existing technologies.
 - **Test Updates** – Evaluate any software or updates in a testing environment and apply patches to production at the firmware, OS, server, client and application levels based on State standards.
 - **Software Version Control** – Follow best practices for software version control to ensure the integrity of all software releases.
 - **Application Updates** – Maintain and deploy changes to system components over internal and/or the public internet as needed for security compliance.
 - **DR Plan Testing** – Perform Disaster Recovery Testing.

- **Performance Monitoring and Management** – Participate in Capacity Planning and Performance Monitoring/ Management activities during development and ongoing operations and maintenance activities, including support for storage location considerations.
- **Data Analysis Support** – Support for State subject matter experts in data analysis and reporting where guidance is needed to understand the system’s data model and available data.
- **Defect Resolution** – Perform Break-fix analysis and correction.
- **Third-Party SW Defect Coordination** – Manage relationships with any COTS software vendors and hardware/IaaS vendors for hardware, infrastructure or software implemented as part of this State solution. The Vendor shall work with third-party vendors to facilitate the correction of defects, where it is the responsibility of a third-party vendor to actually correct the defect and deliver a fix to the Vendor for implementation in the State’s environment.
- **Technical Knowledge Transfer** – Perform knowledge transfer to Operations, Support, and Technical staff.
- **Backup Management** – Perform backups of all systems and servers on a regular basis. Minimally, this shall include daily incremental backups and full weekly backups of all volumes of all systems and servers.
- **External Partners Directory** – Create and maintain a directory of external partners to facilitate communication and information exchange

7.3.4 Release Management Requirements

The Vendor shall implement a formal Release Management process that will cover all major and minor software releases. The State shall work with the Vendor’s modifications to ensure integration with the State and its IT Department’s practices.

- The Vendor shall propose a formal implementation plan for supporting tools and processes and include a formal training plan. Implementation shall occur as part of the setup and configuration of O&M.
- The Vendor shall lead the development of the Release Management Process, including:
 - Release Policy and Planning
 - Release Management Rollout
 - Release Schedule
 - Forward Schedule of Change
 - Help Desk Production Turnover
- The Vendor shall provide the following:
 - **Release Management Process Implementation** – The Vendor shall take a lead role in designing, implementing, and configuring the Release Management tools and processes to support the implementation of the Motor Fuel Tax System and the ongoing operation of the State.
 - **Testing and Release Acceptance** – The Vendor shall perform formal planning for testing, and associated release acceptance criteria shall be developed. These tasks shall be performed collaboratively with the State.
 - **Release Rollout Plan** – The Vendor shall develop a complete Release Rollout Plan for each release of software or new configuration. The plan shall be developed collaboratively with the State support team. The plan shall include, but not be limited to, requirements for communications, preparation, training, knowledge and skills to support the system.
 - **Rollout Plan Execution** – The Vendor is responsible for executing the rollout plan for each release.
 - **Site Readiness Surveys** – The Vendor shall participate in the development and execution of Site Readiness Surveys with the State for each release.
 - **Update Support Documentation** – The Vendor shall be responsible for updating all documentation for each new release. This includes business user, technical, training, and support documentation.

- **Configuration Management Database** – The Vendor shall develop and maintain the Configuration Management Database content throughout the project and update it for every release. The Vendor shall provide the content for the database.
- **Archive and Retire Configurations** – The Vendor shall develop and implement procedures and tools to archive and retire all prior releases and configurations as new ones are deployed.
- **Known Error Log** – The Vendor shall develop a Known Error Log as part of the support documentation using the Knowledge Management System or another tool as approved by the State.
- **Release Installation Procedures** – The Vendor shall develop detailed installation procedures for each release and ensure that the plan and related tools and standard operating procedures (SOPs) have been properly tested.
- **Back-Out Plans** – The Vendor shall develop back-out plans jointly with the State for each release. The Vendor shall ensure that the plan is properly documented and communicated to all participants and that preparation and training are in place in case the plan needs to be executed. Any parts of the plan or related tools that need to be tested shall be tested before the release is deployed.

7.3.5 O&M Staffing Requirements

- The Vendor shall recommend and provide sufficient staffing to support the Motor Fuel Tax System Operations & Maintenance.
- The Vendor shall provide on-site technical and application support staff to augment State technical support staff and function as members of the support team throughout the SDLC and Warranty Period.
- During the Warranty Period, the Vendor shall provide two (2) additional full-time employees responsible for completing Motor Fuel Tax System change requests and performing defect analysis and corrections. The State reserves the right to take over the responsibility of the Vendor’s full-time employees from the Vendor prior to the end of the Warranty Period with a thirty (30) days notification. In such case, a credit for the unused portion of time will be provided to the State.
- The State may request additional support from this team after the Warranty Period.

7.4 Exceptions, Liquidated Damages, Bonding, and SLAs

The Vendor shall meet all of the requirements in this RFP. Exceptions

Exceptions to the State's RFP that have been requested by the Vendor as part of the vendor’s proposal response are automatically rejected by the State. The only exceptions to the RFP will be those that have been negotiated by the State and awarded Vendor as part of a contractual agreement.

7.4.1 Liquidated Damages

1. DeIDOT reserves the right to assess Liquidated Damages (“LDs”) in the event that the Vendor fails to meet the requirements of this RFP, the resulting Scope of Work, or the final agreement. The purpose of LDs is to provide a fair and reasonable estimate of the damages that may result from Vendor non-performance or delay. Vendors should note that LDs will not be construed as a penalty but rather as a means to encourage timely performance and consistent adherence to service levels. The LDs described below will be incorporated into the final contract and may be applied at DeIDOT’s discretion. Implementation / Go-Live LDs
 - General Performance Failures During Implementation
 - First Offense: Written warning.

- Second Offense(at any time during the contract term): 1% reduction of that month's invoice.
- Third Offense (at any time during the contract term): 2% reduction of that month's invoice.
- Fourth Offense(at any time during the contract term): 3% reduction of that month's invoice.
- Each Subsequent Offense(at any time during the contract term): Increase of 1% per occurrence (e.g., 5th offense = 4%), capped at 10% of that month's invoice.
- Failure to Meet Go-Live Date
 - 1st Month Late: 2% reduction of the total contract value per month (or fraction thereof).
 - 2nd Month Late(at any time during the contract term): 3% reduction of the total contract value per month.
 - 3rd Month Late(at any time during the contract term): 4% reduction of the total contract value per month.
 - Beyond 3 Month(at any time during the contract term)s: 5% per month, capped at twenty percent (20%) of the total contract value.

2. Operational / System Performance LDs (Post Go-Live)

- System Availability (Uptime)
 - SLA Target: 99.9% monthly uptime.
 - Below 99.9% but \geq 99.5%: 1% reduction of that month's invoice.
 - Below 99.5% but \geq 99%: 2% reduction of that month's invoice.
 - Below 99%: 5% reduction of that month's invoice.
- Critical Incident Response and Resolution
 - Failure to acknowledge a Severity 1 incident within one (1) hour: 1% reduction of that month's invoice per incident.
 - Failure to resolve a Severity 1 incident within four (4) hours: 2% reduction of that month's invoice per incident.
 - Failure to resolve a Severity 2 incident within twenty-four (24) hours: 1% reduction of that month's invoice per incident.
- Help Desk and End-User Support
 - Failure to meet ticket acknowledgement SLA (95% within two (2) business hours): 0.5% reduction of that month's invoice.
 - Failure to meet ticket resolution SLA (90% within agreed timeframe): 1% reduction of that month's invoice.
- System Data Integrity, Backup, and Recovery

- Failure to meet Recovery Point Objective (RPO) or Recovery Time Objective (RTO): 2% reduction of that month’s invoice per incident.
- Failure to perform required backup or recovery testing (e.g., semi-annual drills): 1% reduction of that month’s invoice per missed test.

7.4.2 Bonding Requirements

The successful proposer may be required to furnish a Performance Bond and/or a Payment Bond, each in an amount equal to 100% of the total contract value, within ten (10) business days following contract award and prior to commencement of any work. The bonds must be issued by a surety company authorized to do business in the State and acceptable to the State. These bonds shall ensure the faithful performance of the contract and payment for all labor and materials associated with the project.

Failure to provide the required bonds within the specified time frame may result in contract termination and forfeiture of any award.

7.4.3 Service Level Agreements (SLAs)

The Vendor shall meet standards for Service Level Agreements (SLA) and related metrics to meet the requirements of the State. Additional SLAs may be included in the contractual agreement between the parties.

The Vendor shall comply with and measure each SLA and provide detailed reports for each calendar month, as agreed upon with the State. Such details shall include all data necessary to fully calculate the SLA results, but at a minimum, shall include total system downtime events such as:

- The date and time of the outage
- The duration of the outage
- The root cause of the outage
- The specific system component that was the cause of the outage
- The total time that the system was non-operational during the month for all causes
- The total time the system was non-operational during the month for unplanned causes (excludes planned system maintenance activities).

The Vendor shall calculate and report monthly availability, excluding any time that the system is unusable due to the following:

- Maintenance time
- Failure by the State’s Internet service provider
- Failure by the State’s provided infrastructure
- Force majeure events
- Any failure in the State IT Department’s hardware, software, or network connection
- Bandwidth restrictions

Service Level Requirements

- System Uptime: 99.99%
- Problem Ticket Acknowledgement: 15 minutes
- Top Priority Problem Resolution: 4 hours or less