112	The Authority shall review and Approve all documents submitted. For documents containing less than 100 pages, the Authority will review and provide comment on preliminary draft documents within fifteen (15) Business Days. For documents containing at least 100 pages, the Authority will review and provide comment on preliminary draft documents within twenty-five (25) Business Days. The Authority shall review and provide comment on all final draft and final documents within ten (10) Business Days. When multiple documents are submitted to the Authority simultaneously, or within one week of each other, the number of Business Days required for review shall be doubled.
113	The Contractor shall provide a Customer Review Form (CRF) with each submitted document. The Authority shall populate the CRF and provide the Contractor with written comments on all submitted documents. The Contractor shall respond in writing to all comments through the CRF. The Contractor may schedule and conduct meetings to clarify and resolve any remaining questions and issues concerning the comments and responses provided. The Contractor shall then prepare a revised version of the document for Approval by the Authority.
114	The Contractor shall submit a hard copy and the electronic version of all Contractor developed documentation for Authority review and Approval unless otherwise directed by the Authority. Acceptable electronic formats are Microsoft Word 2016 (or higher), unsecured and indexed Portable Document Format (PDF), Excel (as appropriate) and professional CAD applications for Contractor-prepared documentation.
115	The Contractor shall update documentation as changes occur through the Implementation Phase and the Operations and Maintenance Phase. All changes shall be submitted to the Authority for Approval. The Contractor shall maintain a document Submittals list on the EDMS identifying all versions of documents, the date submitted, the nature of changes and identify what the changes are within the documentation.
116	All documentation submitted by the Contractor under this Agreement shall be the property of the Authority and shall not be marked with "Proprietary" unless agreed to by the Authority.

4.2. Documents

4.2.1. Quality Plan

The Quality Plan will include details about how the Contractor will plan and implement the QA program, how to address errors (quality-related events) and how to make improvements before an error occurs (continuous quality improvement). The Quality Plan will address all phases and Work.

117	The Contractor shall develop a CSC Operations Quality Plan that details the Contractor's QA program in a concise manner customized to this Project.
118	The Quality Plan shall include the Contractor's QA approach related to overall project management and controls, including but not limited to:
	• quality management and organizational structure;
	• project management;
	• project controls;

	• project documentation and updates and
	• project scheduling.
119	The Quality Plan shall include the Contractor's QA approach related to BOS design and development, operation, Software Maintenance and BOS administration, including but not limited to:
	• overall design;
	• Software development, initial and on-going;
	• Software development standards and documentation;
	• testing;
	• adherence to Security Standards;
	• installation;
	• quality management of all BOS created customer communications and Notifications;
	• adherence to Performance Measures;
	• configuration management;
	• change management;
	• monitoring and administration and
	• BOS installation and operational mobilization.
120	The Quality Plan shall include the Contractor's QA approach related to CSC Operations, including but not limited to:
	• quality management of every CSC Operations function;
	• ongoing Customer Satisfaction Surveying and how the tool and information will be used;
	• customer service quality improvements;
	• adherence to Security Standards;
	• quality management and organizational structure;
	• quality management documentation;
	• Contractor's quarterly audit;
	• all State and Federal audits per the Agreement;
	• all required and Authority led audits;
	• quality review and verification;

	• adherence to Performance Measures and
	• CSC initial and on-going staffing.

4.2.2. Software Development Plan

121	The Contractor shall develop and submit a Software Development Plan (SDP) that includes but is not limited to:
	• documentation of the Software development approach to the application structure, behavior, architecture, business processes and data structures;
	• Software development organizational chart, including resources and responsibilities, such as Software developers (by area of development), system engineers, test engineers, Quality Assurance and Quality Control personnel, configuration management administrator, documentation specialists and management staff;
	• Software development languages, development platforms and standards;
	• Software development methodology, such as use cases, modeling and other development tools;
	• management and control of Software versioning and major releases;
	• description of the Software development life-cycle and Maintenance;
	• location and approach to segregation of development and testing environments;
	• development problem reporting and defect tracking;
	• code reviews;
	• internal testing methodology;
	• regression testing;
	• Software development language strategy related to both development and Software Maintenance;
	• development and integration approach for the major functional Modules;
	• detailed Software Quality Control processes;
	• Software documentation, standardization, review and usability;
	• samples of detailed Software documentation for both external and in-line documentation;
	• Software configuration and change management approach and standards and
	• Software deployment approach, release notes and validation.

4.2.3. Requirements Traceability Matrix

The RTM provides traceability between Requirements and BOS functionality in a matrix format. The RTM shall be the basis for all design, development and testing efforts and documentation to be developed by the Contractor.

122	Upon completion of the BOS Requirements review process the Contractor shall deliver a RTM that details all the technical and functional Requirements for the BOS.
123	The Contractor shall develop and submit an RTM that identifies each Requirement and where it is addressed in the design documents, use cases and test cases, including but not limited to:
	• listing and multiple levels of categorization (e.g., functional, Interfaces, Modules, etc.) of all Requirements;
	• identification of the source of all Requirements;
	• identification of the design section of the SDDD that addresses the Requirement;
	• identification of the test procedures that address the Requirement;
	• Identification of the test method to validate the Requirement (e.g., via inspection, demonstration, analysis, test) and
	• identification of the Business Rules associated with each Requirement.
124	The RTM shall build on the specifications documented in the CSWRD and shall capture all user needs identified during the Requirements review process.
125	During the design and development of the BOS, the Contractor shall update the RTM to reflect any changes to the Requirements and Requirements tracing that have been Approved by the Authority through the Project's change control management process.
126	During design and testing, the RTM shall be used to verify the compliance to the Requirements, use cases and test cases.
127	Upon Approval of the RTM, it shall be the basis for functional verification of design, development and testing.

4.2.4. System Detailed Design Document (SDDD)

128	The Contractor shall develop and submit an SDDD that describes the design specifications of all Hardware and Software provided as part of the BOS to meet the Approved Agreement Requirements. The SDDD shall demonstrate that the Contractor understands the functional, technical and Performance Measures of the BOS and has the processes, system and Software design in place to provide a high-quality and reliable product that meets the Requirements.
129	The SDDD shall be written in accordance with the Quality Plan as defined in Section 4.2.1.

130	The SDDD shall comply with data retention Requirements set forth in the Security Standards and Section 4.2.17 Records.
131	The SDDD shall include the use of diagrams, figures and tables, and it shall apply to all required environments, Contractor-provided systems, and Software to be used by the Contractor, all Interfaces and all Third-Party Service Providers.
132	The Contractor shall work with the Authority's marketing department in developing the Self-Service Website navigation and look and feel.
133	The SDDD shall include but not be limited to:
	• logical BOS diagrams for all environments that identify all subsystems, components, connections and Interfaces;
	• physical BOS architecture diagrams for all environments that identify all sites, Equipment and network layout diagrams;
	• telephony, IVR and ACD system flow diagrams, including call routing options;
	• high system availability design for all BOS components, including servers, storage, network, database and application;
	• detailed desktop computer Hardware, Software and peripheral configurations;
	• access/identity security methodology;
	• network sizing and design details including IP scheme;
	• complete bill of materials, including Hardware, Software and support/Maintenance agreements;
	• specification sheets for all Equipment including space and power requirements;
	• Disaster Recovery and Business Continuity design, including network impacts;
	• detailed database design, schema and entity relationship modeling, including transaction and file sizing and processing calculations;
	• detailed database data dictionary;
	• detailed data management design and processes, including summarizations, archiving and purging;
	• all documentation required under PCI and PII and to document conformance with the Security Standards;
	• Interface Control Documents (ICDs) for all external Interfaces and file upload functionality documenting both sides of the Interface;
	• detailed Software architecture, internal software component interfaces, logic and process flows;
	• detailed transactional and Violation processing logic and flow;

	• detailed financial processing logic and flow, including interface and mapping to the Authority's financial applications;
	• Self-Service Mobile Application (Phase II and optional) flow diagram;
	• Self-Service Website site map;
	• application performance monitoring design;
	• all GUIs (including reports and screen formats);
	• format of all correspondence for all channels and
	• account management design and account types.

4.2.5. Master Test Plan (MTP)

The Contractor shall develop and submit a comprehensive testing plan that describes the different test phases, the Contractor's testing concepts and approach and the administration of each test. The Master Test Plan (MTP) outlines the scope and testing concepts to be used to validate the BOS compliance to the Requirements, including integration to the ETTM System, external entities and Interoperable Agencies, and compliance to all Business Rules and Security Standards.

134	The Contractor shall provide an MTP for the Authority's Approval that details the testing methodology utilized by the Contractor to demonstrate the BOS satisfies all Requirements.
135	The MTP shall cover all aspects of the BOS testing and shall describe all test phases, scope and procedures to validate the BOS compliance to the Requirements, including but not limited to:
	• overall approach to testing, including tools and automation;
	• approach to using use cases and test cases to validate all Requirements;
	• approach to entry and exit criteria;
	• approach/methodology to pass/fail criteria;
	• approach to the severity and priority descriptions and levels for each test;
	• approach to defect tracking; reported; resolution, and regression testing, including tools used to document defects;
	• approach for each test phase including purpose, scope, system environment, duration location, and resources;
	• methodology for testing the Requirements and sample size for each phase of testing;
	• approach for how data sets for each test are created including data needed to simulate logical days and cycles;
	• approach to validating BOS Requirements through the testing methodology;

	• approach to validating Performance Measures;
	• approach to validating all reporting Requirements;
	• approach to end-to-end testing, validation and reconciliation;
	• approach to validating BOS monitoring, logging, access, Performance Management and Monitoring System (PMMS) Requirements;
	• approach to testing, compliance to standards, correction of defects and Software release;
	• end-to-end testing to ensure processes, transactions/trips and their interaction are tested through their final stages or disposition;
	• Interface testing to ETTM System, Interoperable Agencies and Third-Party Service Providers;
	• Security Standards;
	• financial activity and reconciliation;
	• redundancy/failover aspects;
	• DR aspects and
	• cross-channel testing to ensure testing is not only performed for each Interface (such as, Self-Service Website, Self-Service Mobile Application (Phase II and optional), and IVR) individually, but also that testing is performed across each Interface to ensure consistent presentation and processing.

4.2.6. Individual Test Plan and Test Procedures

The Contractor shall develop and submit individual test plans that describe the required test phases, the Contractor's testing concepts and approach for the administration of each test defined later in these Requirements. The individual test plans will provide detailed documentation of the individual testing plan and procedures.

136	The Contractor shall provide a separate detailed test plan for the Authority's Approval for each testing phase outlined in the Requirements and MTP, including:
	• Unit Test Plan;
	• System Integration Test Plan;
	• User Acceptance Test Plan;
	• On-site Installation and Commissioning Test Plan and
	• Operational and Acceptance Test Plan.
	The Contractor shall provide a detailed test plan, including but not limited to:

137	• test agenda including location, dates, meetings, testers, observers and attendees;
	• test scripts for manual and automated tests;
	• detailed use cases and test cases mapped to the RTM for all testing;
	• test entry and exit criteria;
	• test preparation;
	• description of process for ensuring quality of testing and documentation;
	• test data creation process and
	• description of the environment used and Software versioning.
138	The Contractor shall provide use cases and test cases for Authority Approval for each testing phase outlined in the RTM, including but not limited to:
	• use case/test case ID;
	• use case/test case description;
	• mapped Requirements and Business Rules;
	• assumptions:
	• test data (variables and their values);
	• steps to be executed;
	• expected results;
	• pass/fail criteria;
	• space to document actual results and
	• space for comments.

4.2.7. Implementation Plan and Related Documentation

The Contractor shall develop and submit an Implementation Plan and related documentation that identifies its approach that covers the major elements of the implementation, including coordination with the Authority's ETTM System Contractor, Third-Party Service Providers and others.

139	The Contractor shall develop and submit the Implementation Plan that documents all implementation related activities for the Project for Authority's review in accordance with the Approved Baseline Implementation Schedule.
140	The Implementation Plan shall define all elements of implementation, including but not limited to:

	• the detailed implementation schedule, detailing all activities for the implementation of the BOS, including coordination with ETTM System Contractor, Third-Party Service Providers and others as required. Once the implementation schedule is Approved by the Authority, the Contractor shall submit to the Authority updates during the implementation period(s) identifying any proposed implementation schedule changes and Work progress in the form of percentage completions;
	• resource allocation Requirements for all implementation period(s);
	• procurement and installation of the communications network;
	• Quality Control, Quality Assurance, inspection and testing processes;
	• special or unique implementation Requirements;
	• an organization chart with contact information, roles and responsibilities and includes ETTM System Contractor, Third-Party Service Providers and others as required and
	• Go-Live checklist.
141	The Contractor shall develop and submit to the Authority a full size (24" by 36") set of drawings with installation notes, providing sufficient and accurate detail of all systems and network layouts at all facilities that have BOS Equipment.

4.2.8. Disaster Recovery Plan

The Disaster Recovery Plan (DRP) is a comprehensive, documented statement of actions to be taken before, during and after a disaster to protect and recover the information technology data, assets and facilities of the BOS.

142	The Contractor shall develop, test, and submit a Disaster Recovery Plan (DRP) and subsequent Disaster Recovery procedures that describe the approach, as well as procedures to take place in the event of a disaster for the BOS.
143	The DRP shall document the Contractor's approach to and planning for recovering from a disaster, including but not limited to:
	• define what constitutes disaster, associated risks and severity levels and timeframes to address (e.g., earthquake, flood, electrical outage, general loss of access to building, etc.);
	• mitigation of disaster risks;
	• preparations in the event of a disaster;
	• organization chart illustrating Disaster Recovery team members, roles and responsibilities;
	• notification contact list, including contact information;
	• notification protocol;

	• sites and Equipment for Disaster Recovery, presented in a diagram format;
	• Disaster Recovery process initiation and completion checklist;
	• coordination with the ETTM System Contractor and all Third-Party Service Providers;
	• Software, system and data replication processes;
	• detailed logistical processes for activation of Disaster Recovery site and systems;
	• detailed technical processes for activation of Disaster Recovery site and systems;
	• detailed operational functions for activation of Disaster Recovery site and
	• detailed technical processes for reactivation of primary site (or moving to a new primary site if the original primary site is destroyed) for systems and coordination with Authority's operations.
144	The DR shall include the following BOS information, including but not be limited to:
	• Recovery Point Objective (RPO): maximum acceptable amount of data loss for all critical BOS services after an unplanned data-loss incident;
	• Recovery Time Objective (RTO): maximum acceptable amount of time for restoring a critical BOS services and regaining access to data after an unplanned disruption;
	• Level of Service (LOS): the combination of throughput and functionality required to sustain BOS business operations and
	• detailed description of how site and BOS security shall be maintained to ensure continued compliance with the Security Standards.
145	The DRP shall be tested and updated by the Contractor annually.

4.2.9. Business Continuity Plan

The Business Continuity Plan (BCP) is a comprehensive, documented statement of strategy, as well as the planning, actions and processes that allows the Authority to continue BOS and CSC Operations after experiencing a disruptive event.

146	The Contractor shall develop, test, and submit a Business Continuity Plan (BCP) that details the Contractor's approach to accommodating the staffing capabilities, furnishings, Equipment, systems, network, applications and data components required to ensure the continuity and resumption and continuity of critical BOS processes.
147	The Contractor shall be responsible for providing a high-level plan for restoring CSC Operations in the event that facilities become unavailable; however, the plan shall not result in any costs to the Authority for pre-staging of Equipment and personnel.
148	The Contractor shall be responsible for providing a detailed plan for restoring CSC Operations in the event that all or part of the CSC staff are directed by the Contractor or the Authority to work-at-home. For example, during an event similar to the COVID-19 outbreak.

149	Changes to the operations BCP shall be reflected in the BCP within thirty (30) Calendar Days of Approval. The Contractor shall distribute, train and educate the operations staff on the BCP.

4.2.10. BOS Installation Plan

The BOS Installation Plan will be used by the Contractor to successfully install and prepare the BOS for testing and eventual Go-Live.

150	The Contractor shall coordinate with the Authority, Third-Party Service Providers, and the ETTM System Contractor to develop and provide a detailed BOS Installation Plan, subject to Approval by the Authority that identifies all aspects of BOS installation and start-up of all activities and systems associated with the testing and implementation of the BOS in accordance with the Security Standards.
151	The BOS Installation Plan shall incorporate all aspects of the BOS installation, start-up and Go-Live, including but not limited to:
	• approach to installing the BOS, including network Equipment; CSC Equipment and Desktop Environments;
	• communication procedures;
	• BOS licensing;
	• website static content;
	• phone numbers;
	• BOS access control;
	• network addresses;
	• mapping of all start-up activities;
	• approach to compliance with Security Standards during installation and testing;
	• coordination and Interface testing and start-up activities required with the ETTM System Contractor, and Third-Party Service Providers;
	• approach to achieving commencement of Ramp-up/Customer Services;
	• acquisition and implementation of domain names and URLs;
	• installation team organizational structure, roles and responsibilities and
	• other activities required for the Go-Live from a system standpoint.
152	The BOS Installation Plan shall describe the approach to testing support, including but not limited to:
	• approach to the iterative and repetitive testing phases;

	• within each testing phase the approach to resetting account balances, advancing aging and other system administration activities necessary to support repetitive testing and
	• within each testing phase the approach to establishing required Interfaces.

4.2.11. CSC Operations and Facility Mobilization Plan

The CSC Operations and Facility Mobilization Plan shall be developed by the Contractor and shall include an explanation of how the Contractor will manage CSC and CSC facility mobilization.

153	The Contractor shall coordinate with the Authority to develop a detailed CSC Operations and Facility Mobilization Plan that identifies and plans for all activities, data and Authority-owned materials associated with the mobilization of the CSC, as well as all aspects of design and coordination of the CSC and WIC facility.
154	The CSC Operations and Facility Mobilization Plan shall include how the Contractor will stage new operations for testing and Go-Live.
155	The CSC Operations and Facility Mobilization Plan shall address how and where the Contractor will train the staff without disrupting current operations.
156	The CSC Operations and Facility Mobilization Plan shall incorporate all aspects of the CSC Mobilization, including but not limited to:
	• pre-Go-Live account creation and transponder delivery;
	• transponder inventory;
	• Violation work;
	• all printed customer collateral;
	• hardcopy documentation;
	• softcopy information owned by the Authority;
	• mobilization of CSC facilities;
	• post office boxes;
	• Postage meters;
	• phone numbers;
	• staffing for testing;
	• staffing for initial pre-Go-Live marketing period;
	• staffing for initial Go-Live;
	• security personnel as required by Contractor;
	• administration of CCTV surveillance and physical security systems;

	• service contracts;
	• training and
	• Go-Live activities.
157	The CSC Operations and Facility Mobilization Plan shall include a mobilization and facility mobilization and occupancy schedule.
158	The CSC Operations and Facility Mobilization Plan shall be submitted for Approval by the Authority as a part of the Operations Plan in accordance with the Approved Baseline Implementation Schedule.

4.2.12. End of Agreement Transition Plan

The End of Agreement Transition Plan shall address how the Contractor will support the Authority and the Contractor's successor to facilitate a seamless transition upon termination or expiration of the Agreement.

159	The Contractor shall develop a detailed End of Agreement Transition Plan that identifies the transition of all activities and Authority -owned materials and data associated with the Operation of the CSC at the end of the Agreement.
160	The End of Agreement Transition Plan shall incorporate all aspects of the transition, including but not limited to:
	• customer service, billing and violation work in progress;
	• accounts and violations in collections;
	• Merchant Service Provider activities;
	• transponder inventory;
	• all printed customer collateral;
	• all supplies and consumables on hand;
	• hardcopy documentation;
	• softcopy information owned by the Authority;
	• CSCs;
	• staffing;
	• training and
	• Contractor orderly shutdown of non-transitioned items, facilities and services.

161	The End of Agreement Transition Plan shall be submitted for Approval by the Authority as a part of the Operations Plan in accordance with the Approved Baseline Implementation Schedule.
162	The End of Agreement Transition Plan shall be updated and submitted for Approval by the Authority every two (2) years over the term of the Agreement.

4.2.13. Operations Plan

The Operations Plan is a comprehensive source of information about how the CSC will be managed and operated.

163	The Contractor shall develop and maintain a comprehensive Operations Plan that details all aspects of the operation of the CSC, including but not limited to:
	• a description of each department/functional area and providing sufficient detail for the Authority to understand the functions and responsibilities of each department and how it will be staffed, managed and operated;
	• all the Authority's Business Rules and policies related to the CSC Operations;
	• account terms and conditions;
	• detailed SOPs required to operate the CSC;
	• customer data privacy policy;
	• data and physical security including periodic access audit and reporting;
	• human resources and staffing policies and procedures;
	• background check processes;
	• employee code of conduct;
	• Authority's Holidays and hours of operation, including the CSC and other CSC facilities, if applicable;
	• detailed scripts for common customer interactions;
	• copies of each form, spreadsheet, manual tracking sheet, report, letter, email copy, and text copy (BOS and non-BOS generated) which the Contractor will utilize in the operation of the CSC;
	• Quality Control and verification procedures to ensure operations meet the Performance Measures;
	• operations monitoring to ensure compliance with Requirements;

	• a description of how the Contractor will communicate with the Authority pertaining to day-to-day operations and general issues and problems, including but not limited to: Case management, correspondence management, escalation procedures, document control, and Submittals procedures;
	• a description of how the Contractor will communicate with the Authority and Interoperable Agencies in handling customer disputes, dismissals, payments and reconciliation;
	• detailed structure and schedule for monthly Maintenance and operations meetings with the ETTM System Contractor and the Authority (separate meetings or combined at Authority's discretion);
	• emergency response management procedures, including a detailed description of how the Contractor will communicate and respond to emergency conditions and
	• processes and procedures instituted to ensure high customer satisfaction including the details of the Customer Satisfaction Survey Provider Subcontractor and program that will be used to monitor customer satisfaction with the CSC.
164	The Contractor shall provide updates and changes to the Authority no less than annually for Approval and incorporation into the Operations Plan. The Operations Plan shall be a living document and as such, shall be updated and reviewed/Approved by the Authority whenever changes are made to any element of the operations covered in the Operations Plan.
165	The Contractor shall publish a full revision of the Operations Plan no less than annually.
166	The Operations Plan shall be submitted for Approval by the Authority in accordance with the Approved Baseline Implementation Schedule.

4.2.14. Standard Operations Procedures (SOPs)

167	The Contractor shall develop and maintain the SOPs. The SOPs shall use detailed narratives and process flow diagrams in providing step-by-step procedures for every task the Contractor performs. The SOPs shall detail both manual and BOS-aided steps and procedures.
168	Approved, new policies, procedures and changes to existing policies and procedures shall be updated in the SOPs quarterly. The Contractor shall distribute, train and educate the operations staff and the Authority in accordance with the SOPs.
169	The SOPs shall be submitted for Approval by the Authority as a part of the Operations Plan.

4.2.15. Staffing and Human Resources Management Plan

The Staffing and Human Resources Management Plan defines the required human resources needed to meet all of the Requirements for the CSC. It details the selection and assignment of an operations team. It describes how the staff will be recruited, vetted, trained, compensated, evaluated,

disciplined, and terminated. The Staffing and Human Resources Management Plan shall identify the appropriate skill sets and labor to manage the Work and to perform the tasks that produce the specified Deliverables, customer service and performance. It also shall provide for any additional non-labor resources such as tools, Equipment, or processes used by the operations team.

170	The Contractor shall develop a Staffing and Human Resources Management Plan that includes details of the Contractor's staffing program.
171	The Staffing and Human Resources Management Plan shall include a hiring/assignment schedule for anticipated resource Requirements for the duration of the Project.
172	The Contractor shall develop and provide an organizational approach for staffing in the Staffing and Human Resources Management Plan designed to meet the Requirements. This includes but is not limited to:
	• organizational chart with all staff positions (including Subcontractors), head count and reporting relationships;
	• job descriptions for all staff positions by position type;
	• identification of functions which have been subcontracted, the name and responsibilities of the Subcontractor, and name(s) and contact information for Subcontractor's key personnel;
	• description of the process used for determining the appropriate staffing levels for each position;
	• a schedule describing the daily and weekly staff shifts and a description of how the Contractor will adjust staffing to accommodate seasonal and dynamic changes in work volume;
	• recruitment process;
	• background investigation approach;
	• pre-employment testing;
	• training, testing and re-training policies and procedures including refresher and remedial training for both remote and local staff;
	• employee retention and career development program;
	• employee monitoring, performance evaluation and coaching;
	• employee disciplinary process and
	• employee termination process.
173	The Staffing and Human Resources Management Plan shall also include the location of all personnel required to meet Project Requirements (on-site or remote), as well as the Contractor's approach to providing on-site training and support for remote staff.

174	This Staffing and Human Resources Management Plan shall be submitted for Approval by the Authority as a part of the Operations Plan in accordance with the Approved Baseline Implementation Schedule.

4.2.16. Reporting and Reconciliation Plan

The Reporting and Reconciliation Plan shall include a comprehensive, detailed description of actions to be taken and information to be provided to the Authority related to reporting and reconciliation. This document will identify each report and its associated delivery schedule and provide an explanation of the report and its underlying data and how it is used.

175	The Contractor shall develop and submit to the Authority for Approval, a Reporting and Reconciliation Plan that details the Contractor's reporting and reconciliation process.
176	The Reporting and Reconciliation Plan identifies the procedures that the Contractor will use to perform, manage and reconcile all aspects of the CSC. This includes both transactional and financial reconciliation, including allocation of all Contractor's cost and Third-Party Service Provider associated revenue and/or costs.
177	Each reconciliation shall have a separate section which identifies the reports used for the reconciliation, whether or not the report is generated from the BOS, received from a Third-Party Service Provider or (e.g., banks, Collection Agency, Lockbox Service Provider, etc.) or developed manually by the Contractor.
178	The Reporting and Reconciliation Plan shall describe each provided report or report set and the schedule for providing it along with a sample of each report set. This includes but is not limited to:
	• daily reconciliation report;
	• monthly reconciliation report;
	• quarterly reconciliation report;
	• annual reconciliation report;
	• description of Contractor's process for entering, printing and sending refund checks and entering the resulting financial transactions into the Authority's financial accounting systems, including all accounts and processes required to facilitate this entire process;
	• description of financial and cash/check handling controls for the CSCs and
	• other operations and financial reports as needed to fully reconcile and meet the operations Requirements.

4.2.17. Records

179	The Contractor shall meet all data retention Requirements, including durations for retention, as set forth in the Security Standards. The Contractor shall make every effort, within practical business and cost constraints, to purge the personal account information of an account that is closed or terminated. In no case shall the Contractor maintain personal information more than four years and six months after the date an account is closed or terminated. The Contractor shall periodically audit the BOS to verify that it is in conformance with the retention policy.
180	If specific documents or data retention Requirements are not covered in the Security Standards, or the retention Requirement is greater in other applicable Requirements, the Contractor shall maintain records, for the duration of the Agreement period, in compliance with the longer retention period Requirement. Other applicable Requirements include but are not limited to:
	• GAAP;
	• record retention policies for the Authority;
	• IRS Requirements;
	• The California State Archives Data Retention Schedule;
	• all applicable federal, state, local and other laws and regulatory matters and
	• Security Standards.
181	Requirements and standards for records management and retention may change over the term of the Agreement. The Authority will provide any updates to its internal policies and procedures that may impact the CSC records and retention Requirements; however, it is the Contractor's responsibility to ensure it is aware of any changes to relevant standards, statues, and/or rules beyond those of the Authority, and to incorporate such changes in accordance with the provisions of the Agreement.
182	The Contractor shall be responsible for data retention and purging of all paper records, in accordance with the Authority's retention policy and all of the Requirements related to records retention. In the event of a conflict between Requirements, the Contractor shall immediately notify the Authority.
183	The Contractor shall maintain records and data essential to providing objective evidence of quality, and these records shall be made available to the Authority upon request.
184	Quality-related records and data shall include but not be limited to:
	• inspection and test results;
	• records of Subcontractor quality programs;
	• change request documentation;
	• Customer Satisfaction Survey results;

	• operational reviews and walk-throughs and
	• results of internal and Contractor audits.
185	The Contractor shall maintain records in a manner that allows easy access and analysis.

4.2.18. Management Reporting

186	The Contractor shall prepare and submit to the Authority a Monthly Operations Report in an Approved format, on an agreed-upon day each month. This report shall provide the information required for the Authority to verify the Contractor performance as reported by the Contractor, including but not limited to:
	• Project Oversight Report;
	• Contractor Performance Report (including performance against the Performance Measures);
	• monthly operations invoices for the corresponding period;
	• three-month and one-year look forward for budgeted staffing based on estimated volumes;
	• other agreed-to CSC Operations reports;
	• updates to documents and plans which have occurred in the previous month and
	• updated action item list and Approved meeting minutes from the previous month.
187	The Monthly Operations Report package shall detail the Contractor's performance against the Performance Measures (Contractor Performance Report) in tabular and graphical formats. The Contractor shall use reports and other data from operations as Approved, to conduct an analysis of the data and summarize the results. The basis for the data must be the BOS reports and all data must be reconciled against the appropriate BOS report(s).
188	The data shall be presented in a graphical and tabular format showing the Contractor's comparative monthly performance over time.
189	The presentation of the information shall be clear, concise, and professionally organized and formatted.
190	Any failures to meet the Performance Measures shall be identified and details submitted, including the Contractor's plan to correct such occurrences. The associated non-compliance performance adjustment for such failures shall be summarized and tabulated with the total non-compliance performance adjustment provided.
191	At a minimum, the Contractor's Monthly Operations Report shall include the reports listed below; however, the final list of documents to be included shall be developed and Approved as a part of the Operations Plan.

	• Project Oversight Report: This report summarizes the Contractor's Project activities for the reporting period, including major accomplishments, issues and summary reporting. The Project Oversight Report also shall include an updated action items list that tracks all open items to be resolved by the Contractor. The list shall include task description, date created, owner, status, priority, impact/justification, completion due date and notes pertaining to the completion of each task. A status of operational changes shall be included in the Report. The Contractor shall provide status on all existing and new BOS issues that affect operations. The Contractor also shall make recommendations for innovations, processes and BOS improvements and other suggested changes, which will improve customer service or increase operational efficiency.
	• Operations Reports: This suite of reports shall provide the details required to support the Project Oversight Report, including but not limited to: customer contacts, mail handling and Notification response; Case handling; transponder Fulfillment; payments processed; customer disbursements processed; the Authority's and Interoperable Agencies' settlements processed; returned payments processed; chargebacks processed; inventory item Fulfillment and balancing, and reconciliation. Reports related to ongoing Customer Satisfaction Surveys and QA activities and translation services shall also be provided.
	• Refund account reconciliation and request for replenishment: Contractor shall be responsible for issuing customer and violator refunds. Contractor will provide documentation of refunds that were issued. The Contractor shall provide related account and Violation reconciliation reporting to the Authority at least monthly and in accordance with the Operations Plan.
	• Contractor Performance Report: The Contractor shall be fully responsible for the CSC Operations meeting or exceeding required performance. Failure to do so may result in the assessment of non-compliance performance adjustments as set forth in Volume IV Performance Measures. The Contractor shall use the Approved tracking and reporting methods to prove its monthly performance against the Performance Measures.
	• Monthly Operations Invoices: The Authority shall receive a Contractor's invoice for the period corresponding to the Monthly Operations Report. The invoice shall detail the specific amounts due from the Authority. Contractor shall address costs that are netted out from the Contractor's toll revenue payment to the Authority, for example credit card fees and collections fees. Any associated Liquidated Damages shall be separately netted out with detailed supporting documentation. The Authority will not pay operation invoices that are not accompanied by the complete and accurate Approved Monthly Operations Report package.
192	Any performance deficiency the Contractor proposes to have excluded from the non-compliance performance adjustment calculation shall be documented on the Approved Waiver Form and explained in detail, with supporting documentation sufficient for the Authority to make a determination as to the acceptability of the exclusion. If the Authority needs additional information to make a determination the Contractor shall provide such information expeditiously. Adjustments will not be considered until full required documentation is provided by the Contractor.

193	The Waiver Form must be submitted within thirty (30) Calendar Days of the affected invoice in order to be considered by the Authority.

4.2.19. Training Plan

The Contractor shall provide a training program to educate Contractor staff, the Authority and others on the BOS and CSC Operations, as described in Section 5 Training. The Contractor is responsible for providing a Training Plan that describes the approach to training activities.

194	The Contractor shall develop and maintain a Training Plan, subject to Approval by the Authority, in accordance with the Approved Baseline Implementation Schedule.
195	The Training Plan shall describe the plan for training CSC Operations staff and Authority-designated individuals and shall outline the required operational/Maintenance and BOS knowledge for each position to be gained from the training. For each BOS position/user type, the plan shall include a training instructor guide, training manual and other materials to be used in training.
196	The Training Plan shall include a schedule for regular staff training, follow-up training and continuing education for staff.
197	The Training Plan shall describe the approach to training administrators, end users at different levels, Maintenance and support personnel, including but not limited to:
	• overall description of the training program;
	• training techniques;
	• training delivery schedule;
	• how training will occur with staff working on live operation;
	• recurring training through life of the Agreement;
	• names and descriptions of each training class;
	• purpose of each training class;
	• who should attend the class;
	• qualification Requirements for trainer;
	• minimum qualifications for personnel attending the class;
	• duration of the class;
	• training materials, including syllabus, schedule, training goals, manuals, guides, other support materials and techniques to be used;
	• data preparation, such as test accounts and test transactions/trips;
	• required Equipment and

	• facility Requirements.

4.2.20. Maintenance Plans

The Contractor shall develop and submit the Maintenance Plans listed below that describe how the Contractor plans to perform the Maintenance of the BOS and all Hardware, Software and systems at the BOS facilities and CSC throughout the Operations and Maintenance Phase. The Contractor shall have appropriate BOS documentation available to all Maintenance and Software support personnel, as required to perform their respective duties.

4.2.20.1. System Maintenance Plan

198	The Contractor shall develop and submit the System Maintenance Plan that defines the approach to services, staffing and resources to fulfill the BOS Maintenance Requirements. The Contractor shall identify the Contractor's Maintenance responsibilities and shall include but not be limited to:
	• organizational structure, organizational chart and job descriptions and responsibilities;
	• staffing plan;
	• approach to training;
	• detailed BOS monitoring Requirements;
	• staff schedule and locations;
	• third-party system support agreements overview;
	• location of offsite data storage;
	• schedule of all System Maintenance activities, including anticipated Upgrades/Enhancement releases;
	• description of all System Maintenance related communication methods;
	• Maintenance procedures, communication protocols and Approval processes for BOS Upgrades, Software deployments, scheduled Maintenance activities, change management and scheduled downtime;
	• Maintenance procedures and communications protocols for unscheduled downtime;
	• communication protocol for coordination with Interoperable Agencies and Third-Party Service Providers and WICs;
	• communication protocol for coordination with the Authority's other toll system vendors;

	• trouble reporting processes, notification protocols for issues and failures, and Maintenance reporting processes;
	• prioritization, response, escalation, and repair processes;
	• spares levels, Equipment and third-party Software warranty tracking and return material processes;
	• monitoring Maintenance performance for compliance with Performance Measures;
	• sample Maintenance reports and reporting processes;
	• processes for supporting internal and external audits;
	• Security Standards compliance monitoring, Upgrades and safeguards;
	• system intrusion monitoring and safeguards;
	• Equipment replacement/refresh schedule;
	• Upgrades to third-party Software and tools and
	• processes in place to meet Performance Measures.

4.2.20.2. Software Maintenance Plan

199	The Contractor shall develop and submit a Software Maintenance Plan that defines the approach to services, staffing and resources to fulfill the Software Maintenance Requirements and warranty provisions as set forth in the Agreement, including but not be limited to the following elements:
	• organizational structure, organizational chart with job descriptions and responsibilities;
	• staffing plan;
	• approach to staffing and training;
	• approach to receiving and prioritizing Software defects (bugs);
	• reporting, categorization, prioritization and disposition of Software defects;
	• coverage and personnel locations;
	• all Software Maintenance related communication methods;
	• Maintenance procedures, communication protocols and Approval processes for Software Upgrades, scheduled Maintenance activities, change management and scheduled downtime;
	• documented change control procedures;

	• Maintenance procedures and communications protocols for unscheduled downtime;
	• trouble reporting processes;
	• escalation processes;
	• sample Maintenance reports;
	• Software updates to comply with Interoperable Agencies' specification changes and Third-Party Service Providers Interface changes;
	• Software updates to be compliant with Security Standards and
	• processes in place to meet Performance Measures.

4.2.21. Third-Party Documentation

Third-Party documentation includes standard commercial documentation for third-party provided Hardware, Software, services and materials.

200	The Contractor shall provide and maintain standard, commercially available, updated documentation for third-party provided Hardware, Software, services and materials provided under this Agreement. This set of third-party documentation shall be available upon request.
201	An electronic copy of all third-party Commercial Off-the-Shelf (COTS) Hardware and Software installation and user manuals, with updates, shall be provided to the Authority.

4.2.22. Manual Requirements

Various manuals shall be provided to educate and guide BOS administration staff and allow the Authority to understand the operations of the BOS.

202	Whenever possible, all data shall be printed on 8-1/2" x 11" sheets; foldouts shall be 11" x 17".
203	Each manual shall include, but not be limited to:
	• a title sheet;
	• revision history;
	• Table of Contents;
	• list of illustrations (if applicable);
	• list of reference drawings and exhibits (if applicable) and
	• a parts list (if applicable).

204	All manuals shall have a consistent look and feel and shall be professionally written and presented in clear and organized fashion.
205	All manuals prepared for the Authority under this Agreement shall be produced, or editable, using Microsoft Office 2016 Suite (or higher if Approved by the Authority). In addition, electronic copies of manuals shall be provided in unsecured Portable Document Format (PDF), if requested by the Authority.
206	Any special Software required to produce scalable typefaces or other graphs shall be provided by the Contractor as part of the documentation for the manuals.
207	All manuals shall be submitted and Approved as a condition of Go-Live.

4.2.22.1. Manual Submissions and Quantities

208	The Contractor shall submit one (1) hard copy of each of the manuals listed below.
209	The Contractor shall submit electronic copies of all manuals listed below.
210	All manuals shall be maintained in electronic format in the Contractor-provided EDMS.
211	The Contractor shall be responsible for producing an additional quantity of the manuals for the Contractor's use, sufficient to fulfill the Contractor's Requirements.
212	The Contractor shall submit the draft and final manuals described below for the Authority's review and comment, in accordance with the Approved Baseline Implementation Schedule. All final versions of manuals shall be provided and Approved before system Go-Live.

4.2.22.2. Manuals to be Submitted

4.2.22.2.1. BOS User Manuals

213	The Contractor shall develop and submit BOS User Manuals to be used by CSC Operations staff to operate the BOS and for training purposes.
214	The Contractor shall develop manuals logically to cover job categories and functions. The manuals shall detail all of the processes, procedures and policies developed by the Contractor that are required to fulfill the Requirements for each of these categories and functions. An example of a functional area is finance, which should include all basic financial responsibilities and functions, including the entire reconciliation process.
215	Each BOS User Manual shall include but not be limited to:
	• screen images detailing the step-by-step activities needed to fulfill a specific functionality;
	• flowcharts to provide the CSC Operations staff a clear understanding of the workflow;
	• all screens, reports and data fields, clearly explained using sample formats applicable to the BOS and

	• samples of all reports, included in the manual or as an attachment to the manual, with any specific instructions that may apply to a given report.

4.2.22.2.2. BOS Finance and Financial Controls Manual

216	The Contractor shall develop and submit the BOS Finance and Financial Controls Manual, which shall include but not be limited to:
	• detailed descriptions of all procedures to balance and reconcile the BOS;
	• detailed descriptions of Financial Account Posting, reporting and reconciliation to the Authority's Bank Accounts;
	• detailed descriptions of reconciliation of transactions/trips and revenue within the BOS with each of the Interoperable Agencies and for payments made to the Authority and Interoperable Agencies;
	• processes and reports used to reconcile third-party payments processed and money deposited in the Authority's bank;
	• detailed descriptions of reconciliation of all collections activity and all exceptions processing;
	• detailed descriptions of the screens, reports and functions that allow Contractor or the Authority's finance personnel or independent auditors to access, understand and work with all financial aspects of the BOS;
	• complete descriptions of all reconciliation procedures and a non-technical description of the screens, reports and functions;
	• illustrations and pictorial diagrams to demonstrate the step-by-step operations required for performing the balance and reconciliation functions and
	• included as an attachment to the manual, samples of all relevant reports, with any specific instructions that may be applicable to a given report.
217	Reports included in the BOS Finance and Financial Controls Manual shall have correct and accurate data.
218	The BOS Finance and Financial Controls Manual shall be used to train the CSC finance personnel and the Authority's finance personnel.

4.2.22.2.3. BOS Administrator Manual

219	The Contractor shall provide a BOS Administrator Manual that serves as a guide to the overall management and administration of the BOS, and it shall include but not be limited to:
	• detailed Hardware Maintenance activities and schedule;
	• detailed database Maintenance activities and schedule;

	• detailed Software monitoring activities and schedule;
	• detailed monitoring procedures for file transfers and exception handling;
	• detailed procedures and processes for all Maintenance activities;
	• detailed procedures for backup, archiving and purging data;
	• detailed procedures for testing and executing Disaster Recovery and Business Continuity;
	• detailed schedule for all preventative Maintenance activities;
	• scheduled time and maximum run time for all BOS jobs and/or processes;
	• technical contact lists for all third-party technical contacts;
	• technical contact lists for Hardware, Software providers and third-party support agreements;
	• details and copies of all third-party system support agreements;
	• general information, such as Maintenance shifts, code of conduct and other human resource aspects and
	• details of the security access system configuration, user access privileges and controls and user tracking processes utilized to ensure system security and to maintain data integrity.

4.2.23. As-Built Documentation

Prior to the Authority's BOS Final Acceptance of the Implementation Phase, as-built documentation shall be provided that documents the final BOS design and implementation.

4.2.23.1. As-Built System Detailed Design Document

220	After the Approval of the operational test, and prior to the Authority's BOS Final Acceptance of the Implementation Phase, the Contractor shall submit the As-Built SDDD that includes all Software and Hardware changes made during the system development, implementation and testing phases.
221	The Contractor shall submit one (1) hard copy in addition to an electronic version of the As-Built SDDD. Acceptable electronic formats are unsecured Portable Document Format (PDF), Microsoft Office 2016 Suite (or higher if Approved by the Authority) and professional CAD applications.

4.2.23.2. As-Built Drawings

222	The Contractor shall provide the Authority with a complete set of As-Built Drawings, which shall be delivered as one (1) hard copy of the complete sets of drawings. The same shall be delivered in electronic format for all Equipment, network and Hardware installed and furnished as part of the BOS. As material changes are made to the system by the Contractor shall update the As-Built Drawings to reflect the current status.
223	The As-Built Drawing sets shall include but not be limited to:
	• all schematics;
	• logic diagrams;
	• Hardware layouts;
	• wiring diagrams;
	• interconnection diagrams;
	• installation diagrams;
	• cable schedule;
	• Interface details;
	• facility build-out details and
	• network diagrams.
224	The Contractor shall update the latest drawings with red lines as changes are incorporated during the installation process. At the completion of the installation, the Contractor shall gather all red line drawings.
225	The red line drawings shall be verified and incorporated into a final As-Built Drawing package. This final as-built package shall include all updated installation drawings, shop drawings and sketches, plans and other drawing types that were used to install the BOS.

5. TRAINING

The Contractor shall provide comprehensive training for all aspects of the BOS and CSC Operations including training, operational procedures, policies and guidelines, and rules of conduct, including customer Interface. Training shall be delivered to the Authority's personnel and Contractor's personnel. Training shall be ongoing throughout the Implementation and Operations and Maintenance Phases.

226	The Contractor shall be solely responsible for supplying the BOS and all materials necessary to complete the delivery of the training program.
227	The Contractor's program shall include but not be limited to computer instruction, training aids and manuals as required.
228	Contractor's training shall be hands on and use actual BOS Software in the training environment.
229	The Contractor shall produce all training materials, documents and manuals in hard copies.
230	When changes or new functionality is provided in the BOS, the Contractor shall update the training materials and train staff on such changes/new functionality.
231	All Authority training shall include a review and description of each of the appropriate Authority's processes and procedures with actual BOS Software.
232	The Authority shall have the right to attend any training sessions.
233	The Contractor shall provide comprehensive training related to all aspects of the BOS administration, BOS functionally and CSC Operations.
234	The Contractor shall employ a training manager to lead all training courses and subsequent ongoing training activities.
235	The Contractor shall train Authority's staff to view all real-time aspects of BOS processes/queues and CSC Operations statistics/queues, as well as research and report on all aspects of the BOS.
236	The Contractor shall cross-train staff from other areas of operations or management for peak period, emergency or temporary assignments to provide for staff redundancy.
237	The Contractor's training manager shall identify the training needs, plan, design, and develop all the training curriculum and materials for the implementation and management of the CSC's on-going training program. The types of training include, but are not limited to:
	• customer service and integrity skills ("soft skills") training;
	• Authority's FasTrak, Violation and payment processing Business Rules and facility specific information ("content training");
	• different operational and facility characteristics of Interoperable facilities;

	• use of the BOS, including all customer contact systems and any other applicable systems;
	• CSC Operations SOPs and
	• PII, PCI, data and physical security.
238	The Contractor's training program shall include training at different times and for different reasons during the course of the Operations and Maintenance Phase, including but not limited to:
	• new hire – this training provides the new employee a thorough, in-depth training covering all of the skills and information required to fully understand and perform their job;
	• refresher – this training provides additional training focused on topics on which the attendees have been previously trained but which the training manager or other Authority management staff identified as requiring additional training for a group of employees;
	• remedial – this training is individually focused on the needs of a particular employee(s) based on customer satisfaction feedback, management observation or employee request;
	• new job/promotion – this training is required when an employee changes jobs or gains additional responsibilities and
	• new content/program – this training is required when the Authority introduce a new program or makes a significant change to the SOPs or the BOS.
239	Contractor training shall cover all functional areas depending on the specifics of each individual user role and job functions.

5.1. Training Courses

5.1.1. System Operation Overview Course

240	The Contractor shall provide a system operation overview training course for the Authority personnel who require a general understanding of all aspects of the BOS and CSC Operations.
241	The Contractor shall ensure class sizes and the number of training hours provided are sufficient to provide a general understanding of all aspects of the operation.

5.1.2. Customer Service Representative Course

This course is for customer service personnel who need to understand all aspects of the direct customer service.

242	The Contractor shall provide a customer service course for staff that need to understand all aspects of the direct customer service functionality, with focus on contact management, account management, Violations processes, payments, Business Rules, Express Lanes facility characteristics, external facing website, etc.
243	The Contractor shall provide an appropriate number of training sessions for the customer service course, ensuring class sizes and the number of training hours provided are sufficient to provide an understanding of all aspects of the operation related to customer service.

5.1.3. BOS Finance and Financial Controls Course

This course is for financial management and auditing personnel who need to understand all aspects of the Operation, particularly those related to financial accounting, reconciliation, audit, and management.

244	The Contractor shall provide a BOS finance and audit training course for financial management and auditing staff that need to understand all aspects of the operation, with focus on financial accounting, reconciliation, audit and management.
245	The Contractor shall provide an appropriate number of training sessions for the BOS finance and financial controls course, ensuring class sizes and the number of training hours provided are sufficient to provide an understanding of all aspects of the operation related to financial accounting, reconciliation, audit and management.

5.1.4. Operations Management Course

This course is for CSC Operations personnel providing hands-on training on the BOS including performance reporting, including all operational performance monitoring (for example, call queues, call statistics, image review queues, etc.); all BOS monitoring (for example, mail queues, status and quantity of all Notifications pending and sent, transponder Fulfillments, status of Interfaces and file exchanges), and call center and IVR configuration.

246	The Contractor shall provide an Operations Management Course for all personnel who require a detailed understanding of the BOS reporting and monitoring. This course also covers configuration of the telephony system.
247	The Contractor shall provide an appropriate number of training sessions for the Operations Management Course, ensuring class sizes and the number of training hours provided are sufficient to provide a detailed understanding of the operations of the BOS and how to access information and reports from the BOS.

5.1.5. BOS Users Course

248	The Contractor shall provide a BOS Authorized Users training course for all personnel who require a detailed understanding of the operations of the System and how to access information and reports from the BOS on items such as status, alarms, performance, transactions and revenue.

249	The Contractor shall provide an appropriate number of training sessions for the BOS Authorized Users course, ensuring class sizes and the number of training hours provided are sufficient to provide a detailed understanding of the operations of the BOS and how to access information and reports from the system.

5.2. Training Materials

250	All training materials should comply with applicable PCI and PII standards.
251	Draft copies of all training materials shall be submitted by the Contractor to the Authority for review, comment and Approval prior to final printing of quantities required for training.
252	The Authority shall have the right to require the Contractor to provide additional interim drafts at no additional cost should draft training materials submitted not be of adequate quality or have missing or incorrect information.
253	Contractor shall provide regular updates to training materials to incorporate any changes to the BOS or operational processes.
254	For each training course, the Contractor shall provide the materials listed in the following sections.

5.2.1. Instructor Guides

255	The Contractor shall provide an instructor guide for each training course, including but not limited to:
	• course agenda;
	• course objective;
	• procedures for managing a training session;
	• resources and facilities required, including Desktop Environments, power and communications Requirements;
	• detailed lesson plans;
	• a description of training aids and items to aid in on-the-job performance (such as where applicable, pocket guides or reference sheets);
	• tests to be administered to assure satisfactory completion and
	• instructions for using any audio-visual support Equipment or materials.

5.2.2. Training Aids

256	The Contractor shall provide all training aids necessary to successfully complete the course agenda and meet the course objective.
257	The Contractor shall provide a way for all trained personnel to access training documents, aids and tips in an online, electronic format for ongoing reference.

5.2.3. Student Workbook

258	For each course, the Contractor shall provide a student workbook, including but not limited to:
	• course agenda;
	• course objectives;
	• schedule of sessions;
	• copies of all overheads and visuals and
	• lesson outlines and summaries.
259	The Contractor shall supplement the material provided in the student workbook with additional material (as necessary), such as operations and user manuals. If such material is used, appropriate cross-references shall be included in the student workbook to identify the complete set of training materials provided to the student.

5.3. Scheduling and Preparation for Training

260	The Contractor shall provide a minimum two (2) weeks notice to the Authority and work with the Authority on the timing for each training session. The Authority will identify a list of participants the Contractor shall notify to schedule their participation in the training.
261	The Contractor shall perform all scheduling.

6. MOBILIZATION REQUIREMENTS

The mobilization of the BOS and CSC Operations is a major undertaking that will require careful preparation, planning and coordination in multiple functional areas and on many levels to ensure a smooth beginning to operations. The Contractor is responsible for the mobilization in accordance with the BOS Installation Plan and CSC Operations and Facility Mobilization Plan. Close coordination will be required between the ETTM System Contractor, the Authority and the Contractor.

6.1. Operations Mobilization and Facility Coordination

The operations mobilization and facility coordination include all activities necessary to establish and operate the I-405 CSC and WIC in accordance with the Agreement and to coordinate the design of the Authority provided facility. These activities include comprehensive coordination with the Authority, the Authority's design and construction contractors, and other Authority contractors housed at the facility with regards to CSC and WIC design, scheduling of facility occupancy and installation , staff recruitment and training, ordering of supplies, establishment of all necessary services and developing all SOPs for the entire operation. The Contractor shall coordinate with the ETTM System Contractor on applicable portions of the Approved Baseline Implementation Schedule.

262	The CSC Operations Manager and the Mobilization and Facility Coordination Manager shall lead the Contractor's staff in planning and implementing the activities required for operation of the CSC in accordance with the CSC Operations and Facility Mobilization Plan. These tasks include but are not limited to:
	• obtain a thorough understanding of the functions and capabilities of the BOS;
	• produce all required plans and documentation;
	• recruit CSC staff;
	• coordinate with Third Party Service Providers;
	• make any required Approved modifications to the facilities (those required beyond the new facility design inputs provided by the Contractor);
	• plan and conduct training;
	• assist with the selection and implementation of survey solution, IVR, system recordings, Self-Service Website, and Self-Service Mobile Application (Phase II and optional) and
	• meet regularly and coordinate with the Authority, the ETTM System Contractor to perform the Work.
263	The Mobilization and Facility Coordination Manager shall lead the Contractor's staff in planning and implementing the activities related to the new CSC and WIC facility operation of the CSC in accordance with the CSC Operations and Facility Mobilization Plan. These tasks include but are not limited to:

	• meet regularly with the Authority, the Authority's design and construction contractors, and other Authority contractors that will be housed at the facility to plan, provide design input to the new CSC and WIC facility layout, space planning, network, cabling, power, furnishings, physical security, and surveillance CCTV etc.;
	• review and provide comments to all types of CSC plans;
	• coordinate with other contractors and provide a detailed schedule for facility occupancy and facility mobilization and
	• coordinate the procurement and installation of all BOS and CSC Operations network and communications lines with the communications providers.
264	The Contractor shall develop and conduct an Operational Readiness Demonstration and conduct walk-throughs for each facility with the Authority.
265	As an outcome of the Operational Readiness Demonstration and walk-throughs, a punch list shall be developed and resolution of each item Approved by the Authority.
266	The Contractor shall track, status and resolve all pre-mobilization punch list items (as designated and Approved by the Authority) prior to mobilization and track, status and resolve all post-mobilization punch list items (as designated and Approved by the Authority) during the Operations and Maintenance Phase. Until resolved, the status of post-mobilization punch list items shall be provided in all Contractor performance reports and meetings.

6.2. Schedule, Installation and Mobilization

267	The Contractor shall mobilize CSC Operations in accordance with the CSC Operations and Facility Mobilization Plan and the Approved Baseline Implementation Schedule.
268	The Contractor shall install the BOS in accordance with the BOS Installation Plan and the Approved Baseline Implementation Schedule.
269	The Contractor's schedule shall be sufficiently flexible to accommodate modifications or changes, such as early completions or delays in start or completion of dependent work by the Authority and/or the ETTM System Contractor.

6.3. Mobilization of the BOS and CSC Operations

BOS and CSC Operations mobilization includes all activities necessary to begin CSC Operations. The Contractor's Mobilization Manager shall lead the mobilization in accordance with the BOS Installation Plan and CSC Operations and Facility Mobilization Plan and must coordinate with the ETTM System Contractor and Authority to ensure that the mobilization meets the Approved Baseline Implementation Schedule.

270	The Contractor shall manage and conduct mobilization in conformance with BOS Installation Plan and CSC Operations and Facility Mobilization Plan and Approved Baseline Implementation Schedule.

271	The mobilization activities shall be coordinated with the Authority, the ETTM System Contractor, and Third-Party Service Providers, and shall be Approved by the Authority.
272	The Contractor shall prepare internal and external communication procedures, as part of the BOS Installation Plan and CSC Operations and Facility Mobilization Plan, to effectively and professionally manage communications of potential impacts during the mobilization.

6.4. Acceptance of Operational Readiness

Prior to Go-Live the Contractor shall demonstrate to the Authority that the successful CSC and facility mobilization is complete, and that the Contractor is ready to commence complete operation of the CSC and performance of all of the Work.

273	The Contractor shall demonstrate that the CSC Operation has achieved operational readiness in accordance with the Approved Baseline Implementation Schedule.
274	Procedures for demonstrating for the Operational Readiness Demonstration shall be provided by the Contractor to the Authority for review and Approval at least three (3) months prior to the scheduled demonstration date.
275	The Contractor shall have completed all of the predecessor tasks and milestones in the schedule in order to achieve Acceptance of operational readiness, including but not limited to:
	• selection, build-out and equipping of all Contractor operated facilities;
	• development and Approval of all required documentation;
	• recruitment, hiring and training of all staff in accordance with the Operations Plan and sub-plans;
	• implementation of all applicable aspects of the BOS Installation Plan and CSC Operations and Facility Mobilization Plan and all operations mobilization activities and
	• completion of Operational Readiness Demonstration using the BOS, facilities and Contractor staff.

6.5. End of Agreement Transition

The Contractor acknowledges the services it provides under the terms of the Agreement are vital to the successful operation of the BOS and said services shall be continued without interruption. Upon expiration or termination of the Agreement, a successor may be responsible for providing these services. The Contractor agrees to exercise its best efforts and cooperation to affect an orderly and efficient transition to a successor.

As part of the End of Agreement Transition, the Authority may wish to operate and maintain BOS, requiring the transfer of Equipment, leases and license from the Contractor to the Authority.

276	The Contractor shall cooperate with any future transition of the BOS to a future BOS Contractor, as required by the Authority.

277	The Contractor shall develop with the successor, an End of Agreement Transition Plan describing the nature and extent of transition services required as well as the operational Requirements necessary for the migration of operation from the Contractor to the new contractor.
278	The Contractor shall update the End of Agreement Transition Plan no more than six (6) months prior to the transition date.
279	The Contractor shall provide sufficient experienced personnel in each division/element of Work during the entire transition period to ensure the quality of services is maintained at the levels required.
280	The Contractor shall provide sufficient staff to help the successor maintain the continuity and consistency of the services required.
281	The Contractor shall provide the necessary Software and BOS support services to assist the successor in setting up the systems, transferring of appropriate licenses and third-party Software and transitioning all BOS data (including third party data) required to sustain uninterrupted service in areas in which the Contractor is responsible for the Work. For example, accounts and violations in collections.
282	The Contractor shall support the Authority during the procurement process by updating all system documentation and providing new documentation as required that details the current system.
283	Within the End of Agreement Transition Plan, the Contractor shall provide descriptions of the Equipment, leases and licenses that are available for purchase and transfer to the Authority as part of the End of Agreement Transition.
284	The Contractor shall not prevent the successor from conducting interviews with Contractor employees outside of normal business hours in a manner that will not disrupt current operations.
285	The Contractor shall not prevent employees from changing their employment to the successor if the employees wish to do so.
286	The Contractor shall provide for the orderly transition of the facilities, Equipment, materials, documents, inventory and work in progress to the successor.

7. TESTING REQUIREMENTS

7.1. General

The Contractor shall provide the full range of test planning, testing design and services required to ensure the BOS adheres to the Requirements. The BOS testing regimen shall take place during the implementation period identified in the Approved Baseline Implementation Schedule and shall follow the Master Test Plan and Individual Test Plan.

The Authority requires that configuration changes be treated as equivalent to Software development changes within the testing process. Wherever possible, the Authority requires that the Contractor implement testing processes which are automated and efficient.

The Requirements described in this section detail the labor, materials, facility and support services necessary to test the BOS for functionality and performance, its integration to all Third-Party Service Provider.

287	The Contractor shall prepare and conduct the various tests in conformance with the Master Test Plan and applicable individual test plans.
288	The Contractor shall prepare and conduct the various tests (outlined for reference immediately below and with detailed Requirements in subsequent sections), including but not limited to:
	• Unit Testing;
	• System Integration Testing;
	• User Acceptance Testing;
	• On-site Installation and Commissioning Testing and
	• Operational and Acceptance Testing.
289	The Contractor shall develop test scripts for Authority approval and use specialized automated testing Software, wherever possible, to, including but not limited to:
	• create test scripts;
	• create use cases with pre-defined input and output;
	• control the automated testing;
	• exercise all conditions, configurations and scenarios;
	• conduct performance testing;
	• conduct security and PCI testing;
	• conduct regression testing;
	• compare actual test outcomes to expected outcomes;
	• test reporting;

	• conduct load testing;
	• conduct user Interface testing and
	• conduct sustained operational testing.
290	The Contractor shall make the BOS available for use by the Authority in testing the readiness of the CSC Operations staff during operating hours and as necessary during the testing period.
291	The Contractor shall provide all necessary resources and facilities to conduct all tests.
292	During the Implementation Phase, the Contractor shall provide an "online commercial Software" defect tracking system, accessible by the Authority via browser-based internet, to document and track all defects identified as part of BOS testing and any subsequent actions taken to correct those defects.
293	The Authority's Approval of any aspect of testing shall not relieve the Contractor of its responsibility to meet all Requirements.
294	The defect tracking system shall be capable of the following, including but not limited to:
	• rating (severity) defects;
	• categorizing defects;
	• prioritizing defects;
	• logging the date/time the defect was reported;
	• the user who reported the defect;
	• the erroneous behavior;
	• the details on how to reproduce the defect;
	• the developers who worked on the defect;
	• life-cycle tracking and
	• reporting.

7.1.1. Testing Sequence and Logistics

295	The Contractor shall obtain Approval from the Authority and shall have met the entry conditions prior to start of each test, including but not limited to:
	• Approval of all predecessor tests;
	• Approved test procedures for each individual test;
	• Approved test schedule;

	• Approved inventory of test cases and scripts;
	• successful closeout of all outstanding pre-test issues;
	• successful dry run testing with results provided to the Authority;
	• test data set is created and loaded into test environment;
	• submittal of the latest Approved version of the RTM showing test validation against the Requirements and
	• site and BOS are ready to test.
296	After the completion of each test, the Contractor shall submit for the Authority's review and Approval a test report that documents the results of the test.
297	The test report shall include the results of the test; any anomalies and issues identified; comments provided by the Authority; the test data and the corrective action/resolution of each item, and the results of any re-tests necessary to successfully complete each testing phase.
298	The Contractor shall facilitate and support the Authority's participation in the testing and witness each test. The Contractor shall provide the Authority with full access to the test data and results of the test.
299	Testing shall not be considered complete by the Authority until all anomalies and "punch-list" items are closed-out, and the final test report is Approved by the Authority.

7.2. Required Tests

7.2.1. Unit Testing

Unit Testing is defined as a Software testing method by which individual units of source code, sets of one or more computer program Modules together with associated control data, usage procedures, and operating procedures, are tested to determine whether they are fit for use. A unit could be an entire Module, but it is more commonly an individual function or procedure. Unit Testing is the first level of testing and is performed prior to System Integration Testing.

300	The Contractor shall conduct Unit Testing, including but not limited to:
	• testing for all functional elements of the BOS for conformance with the Requirements, Approved design and Business Rules;
	• testing of 100% of all BOS components and negative testing for controlled systems features;
	• testing using actual data generated by the ETTM System Contractor and simulated data as needed;
	• testing with Third Party Service Provider and Interoperable Agencies test environment;

	• testing each Module of the BOS application Software for compliance to coding standards related to screen validations, web navigation, configuration changes, PMMS including all errors, exceptions and failures, backend programs and processes (using simulated data);
	• testing the desktop computer Interfaces and all peripherals;
	• testing of user roles and security elements;
	• all necessary Hardware and Software for the test;
	• all necessary personnel for the test and
	• updated RTM, SDDD, Operations Plan and Business Rules so functionality can be reconciled to the documentation.

7.2.2. System Integration Testing (SIT)

System Integration Testing (SIT), or end-to-end testing, is defined as a type of Software testing that seeks to validate the Interfaces between individual components and the completely integrated BOS meets its Requirements. The Contractor shall conduct SIT, compressing logical days to accommodate process escalation and transaction/trip and Violation aging. Multiple testing cycles may be executed depending on defects found and their severity. The Contractor shall also conduct load/performance testing as part of the SIT

301	The Contractor shall be responsible for creating test data as an entry criteria for the SIT. It is anticipated that significant test data will be required and will be defined in the test plan.
302	The Contractor shall conduct SIT which shall include end-to-end Integration Testing, Interface testing, security testing, performance/load testing.
303	In the event Third-Party Service Providers and Interoperable Agency test environment systems are not available, the Contractor shall test using simulated Interfaces and data to validate the data exchange.
304	The Contractor shall use the most newly provided, developed or updated ICDs for all Interfaces and portals.
305	The Contractor shall conduct SIT, including but not limited to:
	• testing all functional elements of the BOS using the procedures for Software integration testing, including the end-to-end testing from receipt of transactions/trips through Posting to the accounts and Violation processing;
	• reports testing using created data, simulated and keyed-in data;
	• verification and validation that the various BOS environments are operating per the Requirements;

	• load/performance testing of the entire BOS in terms of user access, including internal and external users on all channels (for example, Self-Service Website, Self-Service Mobile Application (Phase II and optional), IVR);
	• load/performance testing of the entire BOS in terms of transaction/trip processing;
	• full Disaster Recovery failover testing;
	• full Disaster Recovery failover recovery (back to primary BOS) testing;
	• validation of all Performance Measures;
	• adherence to the Security Standards;
	• archiving and purging process testing;
	• comprehensive PMMS testing;
	• testing using actual data, generated real-time (as if in a real, live production environment) by the ETTM System Contractor;
	• all Interface test scripts and documentation required to confirm that the Interfaces are operating properly;
	• testing, as directed by the Authority, connecting to test environment systems provided by the Authority, Third-Party Service Providers and Interoperable Agencies (if available);
	• exception testing;
	• testing the desktop computer Interfaces and all peripherals and
	• sustained operations test.

7.2.3. User Acceptance Testing

User Acceptance Testing (UAT) is defined as the testing phase where actual BOS users test the system to validate the operation of the BOS in, according to Requirement, designs, and specifications.

306	The Contractor shall provide all needed support for UAT to include providing environments, provisioning/aging system, running batch jobs, and developing test scripts using use cases.
307	The Contractor shall provide a UAT environment that is production like and separate from other test environments.
308	Ten (10) Business Days prior to the commencement of UAT, the Contractor shall train staff from the Authority and the CSC Operations test team selected to perform UAT.
309	The Contractor shall provide all UAT testers with access to BOS test scripts.
310	The Contractor shall provide test data for UAT that is an extraction and sub-set of production data.

311	During UAT, the Contractor shall develop and retest necessary revisions identified by users during the testing process.
312	The Contractor shall provide technical personnel to support UAT.

7.2.4. Regression Testing

Regression testing is defined as a type of Software testing that verifies that Software previously developed and tested still performs correctly even after it was changed or Interfaced with other Software.

313	The Contractor shall conduct regression testing is to ensure that software changes have not introduced new faults and to determine whether a change in one part of the Software affects other parts of the Software.
314	The Contractor shall conduct regression testing in a Contractor-provided test environment prior to each Software release.

7.2.5. On-site Installation and Commissioning Testing, Mobilization and Go-Live

Onsite Installation and Commissioning Testing is defined as a series of checks and tests to verify Equipment installation and function; BOS operation; and inter-systems operation.

315	The Contractor shall conduct Onsite Installation and Commissioning Testing using the BOS production environment including but not limited to:
	• testing that demonstrates the BOS is completely installed and operational in the production environment and the Disaster Recovery location;
	• Software and test data are loaded;
	• PCI application vulnerability testing, certification of elements not available/tested during previous testing;
	• all necessary Hardware and Software for the test;
	• testing PMMS configuration and setup;
	• testing all user roles;
	• testing of internet connectivity and speed;
	• testing the speed of the BOS while performing various functions;
	• testing of cutover to generator in the event of power failure;
	• testing of phone system including IVR;

	• testing of Self-Service Website and Self-Service Mobile Application (Phase II and optional);
	• all necessary personnel for the test and
	• updated RTM, SDDD and Business Rules so functionality can be reconciled to the documentation.
316	The Contractor shall provide evidence of readiness to conduct mobilization and Go-Live at the BOS production environment, including but not limited to:
	• The Contractor shall utilize the PCI Security Standards Council's Prioritized Approach method to indicate how each PCI Requirement is being addressed. This approach shall be submitted to the Authority along with substantiating evidence for review and Approval;
	• the transfer of certain historical data to the BOS that may remain in the BOS and
	• a checklist to verify that mobilization is completed in accordance with the BOS Installation Plan and CSC Operations Mobilization Plan.
317	Upon Approval of the Onsite Installation and Commissioning Testing including evidence of readiness the Contractor shall begin mobilization.
318	Upon verification and Approval of the Operational Readiness Demonstration and all testing the Contractor shall Go-Live.

7.2.6. Commencement of Ramp-up/Customer Services

Upon Notice to Proceed for Ramp-up/Customer Services, the Contractor is notified of the Authority's intent to Go-Live in approximately 120 days.

319	The BOS shall have achieved commencement of Ramp-up/Customer Services within thirty (30) Calendar Days of the notice to proceed for Ramp-up/Customer Services.
320	The Contractor shall have completed the following tasks to achieve Commencement of Ramp-up/Customer Services:
	• the Self-Service Website is available to facilitate full account creation and transponder ordering (actual shipping of transponders will take place closer to road opening);
	• the Contractor has conducted and successfully completed testing of the Self-Service Website and other functional elements required to facilitate account creation and transponder ordering;
	• the Contractor has gained approval of all BOS design documents;
	• the Contractor has gained approval for all CSC Operations, CSC Facility, mobilization and BOS system installation plans and is on schedule in executing the Approved Plans per the Approved Baseline Implementation Schedule;

	• system support is operational and monitoring the operational components of the BOS and
	• Software support is operational and available to support the operational components of the BOS.

7.2.7. Operational and Acceptance Testing

Operational and Acceptance Testing is defined as a test focused on the readiness of the BOS to be supported, and/or to become part of the production environment.

321	Following Go-Live, the Contractor shall conduct Operational and Acceptance Testing on the BOS production environment in live operations that provides the following, including but not limited to:
	• verification that the Contractor (including the BOS) is compliant with Commencement of Ramp-up/Customer Services;
	• verification that the BOS is in conformance with the Requirements for a period of sixty (60) consecutive days, onsite in the BOS production environment;
	• successful access of images from the ETTM System and receipt of the trip/transactions;
	• reconciliation of all BOS data, transactional and Financial Transactions for a period of sixty (60) consecutive days to verify all data and accounts are being properly processed, reported on and reconciled;
	• reconciliation of all transaction/trip and image workflows and filters to verify all transactions/trips and images are being properly processed through the BOS;
	• reconciliation of all electronic Interfaces and portals, including Third-Party Service Providers and Interoperable Agencies;
	• reconciliation of all account Postings, Financial Transactions, events, etc., to account history entries;
	• reconciliation of all Financial Accounts in the BOS for two (2) monthly financial periods;
	• archiving and purging process testing;
	• disaster recovery testing;
	• verification of PMMS operations;
	• adherence to required financial audit and reconciliation Requirements and
	• adherence to required BOS Performance Measures and reporting.
322	The Contractor shall identify all anomalies and categorize by severity and priority, and all anomalies shall be addressed to the satisfaction of the Authority.

323	If anomalies are identified that are a high severity and high priority during the testing period, the Operational and Acceptance Testing for those functions and any other impacted functions or test areas shall be restarted and shall continue for sixty (60) consecutive days from the day the test was restarted.
324	The Operational and Acceptance Testing shall continue until all the Requirements have been verified and validated in accordance with the MTP and detailed test procedures are completed and Approved by the Authority.

7.3. BOS Acceptance

325	Upon the successful completion and Approval of the Operational and Acceptance Testing, the closure of all punch-list items and completion and submission and Approval of all items required for phase closeout, as set forth in in the Agreement, the Contractor shall be given the Acceptance for the BOS Implementation Phase.

8. INSTALLATION REQUIREMENTS

This section details the Requirements for the installation or enablement of the BOS at the primary and Disaster Recovery/Business Continuity sites as Approved by the Authority.

8.1. Installation Program

The Contractor shall develop and provide an installation program or provide service documentation that addresses all aspects of the installation or use of the BOS, including all installation design, submissions and coordination for a COTS based solution or service agreements for cloud-based approaches.

326	The Contractor shall be responsible for the design, procurement; installation; cabling; configuration; checklist walk-through, and testing of all Hardware, Software, Equipment, Interfaces and communications provided as part of the BOS, if required.
327	The Contractor shall install or enable the BOS at the primary site and CSC locations which meets the specifications outlined in the Requirements and the Approved BOS Installation Plan.
328	The Contractor shall install or provide the Disaster Recovery BOS and Business Continuity at a location which meets the specifications outlined in the Requirements.
329	The Contractor shall provide, install or enable and secure all communication lines required for the primary BOS facility, the Disaster Recovery and Business Continuity facilities and Authority's CSC locations.
330	The Contractor shall provide, install or enable and secure connection points to the BOS as required to accommodate access and communication with Interoperable Agencies and Third-Party Service Providers.

8.2. Compliance to Standards

331	The Contractor shall adhere to all implementation standards, applicable laws, ordinances and codes as required, including but not limited to:
	• the Security Standards;
	• those from the original Equipment manufacturer;
	• the National Electric Code (NEC);
	• the Institute of Electrical and Electronics Engineers (IEEE);
	• the Occupational Safety and Health Administration (OSHA);
	• county and city codes, as applicable and
	• the State of California, for areas including but not limited to electrical codes, seismic considerations, calibration, configuration and environmental.

8.3. Equipment Installation Requirements

The Contractor shall be responsible for installation of the BOS, including at the CSC and WICs, as described in these Requirements.

332	The Equipment installation design and implementation for the BOS and CSC Operations shall include but not be limited to:
	• all Contractor provided Equipment, including desktop computer environments and phone systems for two (2) permanent Authority personnel, and desktop computer environments and phone systems for an additional three (3) oversight personnel during the mobilization of the facility through Operational and Acceptance Testing;
	• Interface with and electronically monitor via the PMMS any Authority or Contractor provided emergency power generation at the I-405 CSC and WIC;
	• furnishing, installing and testing the Interfaces and connectivity between the CSC facility and the BOS;
	• furnishing, installing and testing the Interfaces and connectivity to the ETTM System;
	• validating the connectivity to all Interoperable Agencies as described in these Requirements and
	• validating the connectivity to all external Interfaces to Third-Party Service Providers as described in these Requirements.

8.4. Implementation Checklist Review and Check-off

The Contractor shall complete all implementation activities and Approved Contract Deliverables Requirements prior to the Go-Live date established by the Authority.

333	The Contractor shall develop a checklist that tracks the progress and completion of all implementation activities for the BOS, CSC Operations and Disaster Recovery.
334	The checklist shall detail those items required to complete the implementation process for all Hardware, Software, Equipment, Interfaces and communications provided as part of the BOS, including terminations and connections.
335	The checklist shall be used to identify all discrepancies and exceptions, and the Contractor shall be responsible for all corrections.
336	The checklist shall be used to document all changes identified, and all such changes shall be Approved by the Authority.
337	A representative(s) from the Authority shall have the right to observe and Approve the implementation.
338	The Authority shall have the right to perform independent inspections, and the Contractor shall be responsible for the correction of all discrepancies and deficiencies identified during the inspection.

339	A copy of the checklist, signed and Approved by the Contractor, attesting to the completeness of the implementation, shall be provided to the Authority upon the completion of the implementation activities.

9. GENERAL MAINTENANCE AND SOFTWARE SUPPORT SERVICES REQUIREMENTS

9.1. Operations and Maintenance Meetings

9.1.1. Monthly Performance Review Meetings and Reporting

The Contractor shall conduct Monthly BOS Performance Review Meetings with the Authority. These meetings shall provide the Authority with a detailed understanding and review of the Contractor's and the BOS's performance for purposes of receiving guidance from the Authority, Authority oversight, work planning and invoicing.

340	The Contractor shall manage, facilitate and conduct Monthly BOS Performance Review Meetings with the Authority throughout the Operations and Maintenance Phase. At a minimum, the Project Manager (Implementation Phase), Project Manager (Operations and Maintenance Phase), Software Development Manager and a Contractor's CSC Operations Manager (in-person) shall attend these meetings.
341	The Contractor shall schedule and conduct the Monthly BOS Performance Review Meeting with the Authority to occur no more than one (1) week after the submission of a Monthly BOS Report package by the Contractor.
342	Performance reviews, including the provision of all required performance reporting, shall be provided by the Contractor to the Authority beginning one (1) month after Go-Live for the previous month. Any trip volume fee adjustments associated with non-performance shall not be assessed until the fourth month following Go-Live, for the previous (third) month's performance; however, this does not relieve the Contractor of required performance prior to the third month and shall not constitute a waiver of any Authority rights or remedies under the Agreement in this regard.
343	The Contractor shall ensure all issues are addressed and resolved or are placed on the action item list and scheduled for resolution.
344	In addition to other invoicing and payment Requirements, the Contractor shall provide the required monthly performance reports to the Authority, including all required information demonstrating actual performance relative to the Requirements, before an invoice shall be considered for payment. The monthly performance reports structure shall be identified in the Maintenance Plan.

9.1.2. Monthly BOS and Operations Coordination Meetings

During the Operations and Maintenance Phase, the Contractor shall conduct bi-weekly meetings to coordinate the ongoing operation of the CSC. The Contractor shall be responsible for scheduling these meetings and topics for the meeting shall come from the Contractor; the Authority may provide additional topics. The Authority may attend these meetings at its discretion.

345	The Contractor shall manage, facilitate and conduct the Monthly BOS and Operations Coordination Meetings with the Authority during the Operations and Maintenance Phase in order to understand and prepare for supporting the resolution of BOS-related and Toll Facility related issues and other activities which will affect the CSC Operations.
346	During the Monthly BOS and Operations Coordination Meetings, the Contractor shall address BOS and operational topics for which input is needed from the Authority, including but not limited to reviewing the Contractor's defect tracking report and prioritizing fixes; coordinating Upgrades and Enhancements Approved by the Change Control Board (CCB); reviewing Security Standards and compliance; coordination of scheduled BOS downtime; resolving issues related to personnel and reviewing the Contractor's CSC and WIC support.
347	The Contractor shall identify all known BOS and operational issues and required discussion topics and provide them to the Authority in advance of the meeting and update the agenda again just prior to the meeting.

9.1.3. Weekly Coordination and Status Meeting with the ETTM System Contractor

During the Operations and Maintenance Phase, there will be a series of working meetings between the Contractor and the ETTM System Contractor to provide details on new and open issues and work through possible solutions. The Contractor shall be responsible for coordinating and scheduling these meetings and topics for the meeting shall come from the Contractor, the ETTM System Contractor and the Authority.

348	The Contractor shall manage, facilitate and conduct the Weekly Coordination and Status Meeting with the ETTM System Contractor. These meetings shall be for the purpose of coordination on all new and ongoing issues. The Authority shall be invited to attend these meetings.
349	During the Weekly Coordination and Status Meetings, the ETTM System Contractor shall review the accuracy and sufficiency of reports, review any discrepancies, and to coordinate any changes to the BOS or ETTM System (such as, bug fixes, Upgrades and Enhancement).
350	The Contractor shall identify all known BOS, ETTM System and operational issues and required discussion topics and provide them to all attendees and the Authority in advance of the meeting and update the agenda again just prior to the meeting.

9.1.4. Change Control Board Meetings

During the Operations and Maintenance Phase, the Contractor shall conduct the CCB Meetings. The Contractor shall be responsible for conducting and scheduling these meetings in accordance with the Authority developed change control process.

351	The Contractor shall manage, facilitate and conduct CCB Meetings with the Authority (meeting may be combined with the ETTM System Contractor CCB meeting at the Authority's discretion) on an as-needed basis. These meetings shall be for the purpose of providing status, reviewing, Approving and prioritizing BOS changes (such as, Software enhancements, Software Upgrades, Hardware Upgrades, major bug fixes) and operations changes (such as, policies, Business Rules, operational procedures, phone scripts, and staffing).
352	The Contractor shall solicit and identify all known statuses and input from the Authority regarding the CCB and provide them to all attendees and the Authority in advance of the meeting and in accordance with the Authority's change control process.

9.2. Safety

353	The Contractor shall adhere to all applicable safety standards and guidelines for working on or around energized equipment, including but not limited to the following:
	• The Authority's safety procedures and guidelines;
	• local code;
	• State of California, code, standards, safety procedures and guidelines;
	• Occupational Safety and Health Administration (OSHA);
	• National Electrical Manufacturers Association (NEMA) and
	• National Electrical Code (NEC).

10. CONTRACT DELIVERABLES REQUIREMENTS LIST

The following table identifies the Deliverables/Submittals which shall be required for this Project. This table is provided for convenience only; it is the Contractor's responsibility to meet all Requirements.

CDRL ID	CDRL Name
1.	Project Management Plan (including Baseline Implementation Schedule)
2.	Quality Plan
3.	Software Development Plan
4.	Requirements Traceability Matrix
5.	System Detailed Design Documents
6.	Implementation Plan and Related Documentation
7.	Disaster Recovery Plan
8.	Business Continuity Plan
9.	BOS Installation Plan
10.	CSC Operations and Facility Mobilization Plan
11.	End of Agreement Transition Plan
12.	Operations Plan
13.	Standard Operating Procedures (including BOS and CSC Operations)
14.	Staffing and Human Resources Management Plan
15.	Reporting and Reconciliation Plan
16.	Training Plan
17.	Maintenance Plans (including System Maintenance Plan and Software Maintenance Plan)
18.	Third-Party Documentation
19.	Manuals
20.	As-Built Documentation
21.	Master Test Plan
22.	Unit Test Plan
23.	System Integration Test Plan
24.	User Acceptance Test Plan
25.	Full Software Integration Testing Documentation (includes Approval of all associated updated documents: SDDD, Requirements Traceability Matrix and Business Rules documents)
26.	Onsite Installation and Commissioning Test Plan

CDRL ID	CDRL Name
27.	Operational and Acceptance Test Plan
28.	Training Materials and Manuals

Exhibit B

Volume II: BOS Technology and Functionality

CONTENTS

FIGURES

TABLES

1. STATEMENT OF WORK AND REQUIREMENTS

The following subsections describe the Statement of Work and the Requirements for the Back Office System (BOS). These Requirements are numbered to track obligations per the Agreement and any changes which may occur during the Project. Many of the Requirements contain underlying lists of specific items and required database fields. The intent of these "including but not limited to" lists is to indicate to the proposer the intent and scope of the Requirement. During design, the naming and number of items and fields will vary; however, all items and fields shall be addresses by the BOS unless the Contractor is formally relieved of the Requirement by the Authority.

1.1. Global System Requirements

The global System Requirements define the overarching Requirements for the Hardware, Software and system comprising the production and non-production environments of the BOS.

The Contractor is encouraged to provide innovative solutions that simplify Maintenance, security and the implementation of Upgrades and Enhancements. The Contractor is permitted to use cloud-based and/or premise-based solutions. During the Operations and Maintenance Phase, the entire technical solution and all Third-Party Service Providers must reside and perform the services within the continental United States.

The Contractor will be responsible for acquiring and maintaining the applicable Payment Card Industry (PCI) Standards Security Council Level based on the quantity and value of Credit Card transactions processed. The global System Requirements include Requirements for securing PII in accordance with California statutes, the Authority's privacy policy and National Institute of Standards and Technology (NIST) best practices for general information security.

Connecting the BOS to the Electronic Toll and Traffic Management (ETTM) System, Interoperable Agencies inside and outside California and to Third-Party Service Providers requires a wide variety of external Interfaces. Providing for these Interfaces will require the Contractor to use existing Interface Control Documents (ICD) when applicable and develop new/more modern Interfaces at the Authority's direction.

Although the initial implementation of the BOS will directly support OCTA's I-405 Toll Facility, the BOS design, data schema, financial accounting and reporting approach shall support the future, potential direct support of additional OCTA and non-OCTA Toll Facilities. All functionality provided shall be easily Configured to support these potential additional Toll Facilities.

A BOS-provided Performance Management and Monitoring System (PMMS) shall monitor the performance of the BOS and provide incident and work order management capabilities and data points for measuring the Contractor's Operations and Maintenance Phase performance as further detailed in the Maintenance and Software Support Services section of these Requirements.

1.1.1. Environments

The BOS shall include multiple environments as required to complete the design, development, integration, testing, delivery and Acceptance of the BOS and properly operate during the Operations and Maintenance Phase. It is the Contractor's responsibility to provide additional Authority-Approved environments should the ones listed herein be insufficient for the Contractor to deliver the appropriate solution.

1	The operating environment of the BOS shall include, but not be limited to:
	• the primary BOS;
	• a secondary instance of the BOS to be used for Disaster Recovery (DR) and to support Business Continuity;
	• telephony system;
	• the Interactive Voice Response (IVR);
	• Automatic Call Distribution (ACD);
	• systems for all servicing all channels of customer communication;
	• Desktop Environments installed at the I-405 CSC and WIC Facility;
	• all necessary and required office Equipment (for example, printers, copiers and postage machines);
	• Desktop Environments and telephony systems for two (2) permanent Authority offices throughout the Term of the Agreement. The telephony systems and Desktop Environments shall include full BOS access and supervisory/manager capabilities related to all customer service communication channels and CSR monitoring applications, and one (1) shared private printer for Authority use;
	• Desktop Environments and telephony systems for three (3) additional temporary Authority offices/cubicles during mobilization of the Facility and throughout Operational and Acceptance Testing. The telephony systems and Desktop Environments shall include full BOS access and one (1) Desktop Environment and phone system shall include supervisory/manager capabilities related to all customer service communication channels and CSR monitoring applications (in addition to the two (2) permanent Authority offices Desktop Environments and telephony systems);
	• initial setup, security, and Interface of the I-405 BOS application on desktop computers and peripherals at the OCTA Store WIC (desktop computers and peripherals at the OCTA Store WIC are provided by the Authority);
	• all network and communications elements;
	• all required Interfaces and
	• a data warehouse (Phase II and optional).
2	The primary BOS server environment shall be located at one or a combination of the following locations:
	• hosted at a Tier 3 data center facility and
	• hosted on a well-established cloud service provider.

3	The primary BOS server environment shall have a dedicated infrastructure such that while hosted at a Tier 3 data center facility or by a well-established cloud service provider, the Authority's dedicated BOS application shall run on dedicated virtual machines and/or containers such that only upgrades to the data center/cloud infrastructure and the Authority's BOS application would potentially affect the uptime of the BOS and there is no possibility of functional or infrastructure upgrades required to service other toll customer's applications would cause any downtime or affect the BOS in any way.
4	The Contractor shall ensure the BOS is fully operational in accordance with the Performance Measures described in these Requirements, for the Implementation and Operations and Maintenance Phases.
5	The Contractor shall provide all computing environments required to achieve Commencement of Ramp-up/Customer Services, including but not limited to:
	• a production environment located within the continental United States and
	• a DR environment at a secondary location within the continental United States in a different time zone, or cloud-based equivalent;
6	The Contractor shall provide all computing environments required to sustain the day-to-day operations of the BOS by the Go-Live date, including but not limited to:
	• a production environment located within the continental United States;
	• a DR environment at a secondary location within the continental United States in a different time zone, or cloud-based equivalent;
	• a training environment located at the CSC location;
	• a test environment and
	• a development environment.
7	During both the Implementation Phase and the Operations and Maintenance Phase, the Contractor shall not allow any Authority data or customer PII outside of the U.S. Individuals and entities outside of the U.S. shall only have access to the development environment and shall not have access to customer PII.
8	The Authority shall have logon access to all BOS environments.
9	The Contractor shall keep all BOS environments current with all major releases of operating systems, databases, Software and firmware. Releases shall not be more than one (1) release behind the manufacturer's latest major release unless Approved by the Authority. The Contractor shall also make the necessary Software changes required to ensure compatibility with the evolving IT environment.

10	With the exception of the development and test environments, which may change as part of testing and development cycles, the Contractor shall keep operating systems, databases, Software and firmware consistent across all environments, including, but not limited to configuration and patch level. At least one development and one test environment shall mirror the current production environment at all times during the Operations and Maintenance Phase.
11	The test environment shall be sufficiently sized to successfully test Software changes and their effect on the production environment, including load and stress testing.

1.1.1.1. Operating and Computing Environments – Production

The Contractor is expected to provide a BOS solution that is a dedicated, hosted and/or cloud-based system and as such should provide for the following operating and computing environment Requirements for production.

12	The BOS production environment shall use new Hardware and Equipment for any Equipment installed on-premise at Authority's facilities or at a hosting facility.
13	The BOS production environment shall be a high availability fault-tolerant design configuration of servers, storage, databases and backup systems and connected using high-speed inter-system storage and networking fabric, including any ancillary Equipment necessary to provide a complete production system which meets the Requirements.
14	In the event of a complete failure of one or more of the components or sub-systems in the BOS production environment, affected components or sub-systems shall failover to the secondary BOS at the DR site. Performance and availability Requirements for the individual components and sub-systems of the BOS shall not be affected.
15	The design and implementation of the BOS production environment shall ensure no single-point-of-failure exists within the configuration and the BOS shall continue to operate without data loss in the event any single component of the configuration fails.
16	The operating system used for all servers shall be a multi-user and multi-tasking operating system from a manufacturer that is widely recognized and used in the United States for complex, high-volume database operations.
17	The operating system shall be compatible with all Hardware, Software and other BOS components for the duration of the Operations and Maintenance Phase, including but not limited to:
	• the Relational Database Management System (RDBMS);
	• the Contractor's application Software;
	• the Contractor's proposed network and communications topology and
	• all Desktop Environments and peripherals defined in these Requirements.
18	The operating system shall fully utilize the high availability BOS server architecture.

19	The operating system shall be the latest stable version at the time of implementation (unless otherwise Approved by the Authority), field-proven and have a clearly documented Upgrade path and be supported by the manufacturer.
20	The Contractor shall provide a highly reliable and secure RDBMS for the storage of images, user accounts, transaction/trip data, Violation data and all other data.
21	The RDBMS shall be the latest version at the time of implementation (unless otherwise Approved by the Authority and field-proven to operate in a complex, high-volume transaction environment.
22	The RDBMS shall be certified with the operating system, appropriate application Software and shall fully utilize the high availability BOS server architecture.
23	The RDBMS shall support Upgrades to the operating system, applications, memory, processors and other components.
24	The RDBMS shall have a clearly documented Upgrade path and be supported by the manufacturer.

1.1.1.2. Operating and Computing Environments – Disaster Recovery (DR)

25	For DR purposes the Contractor shall provide a DR computing environment of equivalent size and capabilities to the primary BOS, at a secondary location within the continental United States and in a different time zone from the primary BOS.
26	The DR environment configuration shall continuously mimic the BOS production environment in terms of configuration and data and shall be capable of performing all functions of the production environment, at the same performance and availability levels described in these Requirements for the primary BOS.
27	When put into production, the bandwidth provided to the DR site shall provide for the same performance and reduction of latency as the production BOS for both customers and CSC Operations staff.
28	The DR environment at the DR site shall be capable of being brought on-line and made fully operational in accordance with the Performance Measures.
29	In the event of a catastrophic failure of the primary BOS, the secondary BOS at the DR site shall be capable of sustaining BOS operations indefinitely, or until such time as the primary BOS can be brought back on-line or a new primary site is identified and made fully operational.
30	The Contractor shall provide validation that the DR procedures and environment is capable of providing Business Continuity in the event of a catastrophic failure of the primary BOS. This testing shall be coordinated with the Authority and all the results shall be immediately provided to the Authority.
31	The DR server environment shall be located at one or a combination of the following locations:
	• a Tier 2 data center facility and

	• a well-established cloud service provider.

1.1.1.3. Operating and Computing Environments – Data Warehouse (Phase II and Optional)

The data warehouse provides for the running of data analytics (Business Intelligence) reporting. It also allows the Authority to either directly or upon request to the Contractor, query data and run reports without having to compete for production reporting resources. The data warehouse environment stores all required data (to be defined during the Implementation Phase) from the BOS.

32	The Contractor shall provide, as part of the production environment, a separate data warehouse environment for business intelligence and analytics reporting.
33	The data warehouse shall be dedicated, and the required general reporting shall not depend on the data warehouse in any way.
34	The Contractor shall be responsible for the design and testing of the extract, transform and load (ETL) process from the BOS during the Implementation Phase and the transfer of data after Go-Live throughout the Operations and Maintenance Phase.
35	The Contractor shall provide validation that all data transferred to the data warehouse is complete and accurate.
36	The data warehouse environment shall be updated from production in near-real time.
37	The data warehouse environment shall be capable of being updated via an ETL process from the production System via a one-way replication.
38	Because the data warehouse is Phase II functionality, if the option is executed, at start-up of the data warehouse the Contractor shall extract all applicable historical data from the BOS. The design of the data warehouse database schema, ETL process and the data analytics application shall be part of a post Go-Live, Phase II task.

1.1.1.4. Operating and Computing Environments – Training

39	The Contractor shall provide a non-production training environment, independent from the production and DR environments, to support the initial and ongoing training of the CSC Operations and Authority's personnel.
40	The training workstation environments shall be located at the CSC site unless the Contractor can submit and gain Authority's Approval of an alternative location.
41	The training desktop environment shall replicate the production Desktop Environments, including all peripherals as dictated by the position being trained.
42	The number of training stations shall be determined by the Contractor to meet the training needs in accordance with the CSC Operations and Facility Mobilization Plan and on-going remedial and new training of personnel.

43	The Contractor shall provide the capability to restore training environment databases and to periodically refresh the training environment data from the production BOS, using data cleansing procedures Approved by the Authority.

1.1.1.5. Operating and Computing Environments – Test

44	The Contractor shall maintain a BOS test environment that matches the BOS production environment configuration for the purpose of testing and verifying software Enhancements and Upgrades prior to being put into production.
45	At the Authority's request, the Contractor shall provide access to the test environment for independent testing and verification to software Enhancements and Upgrades prior to being put into production.
46	To the extent possible, the test environment shall interface directly to Third-Party Service Providers and Interoperable Agency test and/or production systems. For example, the DMV and ROV Interfaces.

1.1.1.6. Email, Chat, Fax and Text Messaging

47	The Contractor shall provide the capability for manual, scheduled and system triggered outbound/inbound email (including email attachments) and texting that meets the outbound/inbound correspondence Requirements.
48	The Contractor shall provide the capability for outbound/inbound fax that meets the outbound/inbound correspondence Requirements.
49	The Contractor shall provide the capability for chat sessions that meets the Requirements.
50	The Contractor shall provide the capability for multiple outbound domain name emails to avoid spam blocks or may provide an alternative solution.
51	The Contractor shall provide the capability for Authorized Users to view system-generated status information for electronic messages (such as, email, texting or fax) that are sent from within the BOS application. For example, an Authorized User (e.g., customer service representative) verifies that email messages have been successfully sent from the BOS.

1.1.1.7. Hardware, Software and Other Equipment

52	The Contractor shall provide completely new Desktop Environments for all CSC Operations personnel.
53	The Contractor shall integrate with the BOS all Authority provided or procured 6c transponder readers/programmers for use in the CSC.
54	The Contractor, with the Approval and assistance of the Authority, shall procure any 6c readers/programmers required for the CSC on a cost pass-through basis.

55	All Hardware and Software shall be new, commercially available products currently in production, of the latest design/version at the time of purchase (unless otherwise Approved by the Authority) and field-proven in high-volume revenue operations, including but not limited to:
	• Hardware;
	• Software;
	• firmware and
	• other supplies, Equipment or components.
56	All Hardware and Software shall be obtainable from multiple sources readily available to the Authority, unless otherwise Approved by the Authority. An exception to this may be the Contractor's custom-developed Software.
57	The Contractor shall provide a dated invoice for all materials procured under this Agreement. Shipping bills shall be retained and copies furnished to the Authority along with the invoice on which they appear.
58	All commercial Software provided as part of the BOS shall be enterprise class. Enterprise class applications are designed to be robust and scalable across a large organization and are customizable to meet the specific needs of the BOS. Note: Do not construe this to require enterprise level software licenses. It is the Contractor's responsibility to provide the proper level of software licensing.
59	The solution furnished and installed shall be appropriately sized for capacity, as required to support growth in traffic volumes. It also shall be scalable, allowing for additional transactions/trips, images and Toll Facilities to be added for all BOS functions while continuing to meet the Performance Measures.
60	The Contractor shall use field-proven Hardware, Software and Equipment configurations that support future Upgrades to processors, memory, storage, operating system, database and other system components.
61	Licenses and Software media (or online access for downloading media) shall be provided to the Authority for all Hardware, third-party Software and firmware procured, furnished and installed as part of the BOS.
62	The Contractor shall retain authorized copies (backups) for all Software media as required for use in periodic BOS Maintenance, Upgrades or system restores for a minimum of one year.
63	All Hardware and Equipment provided to support BOS and CSC Operations shall be networked and fully integrated with the functional BOS (including PMMS) and the Desktop Environments.

64	The standard Point of Sale devices shall support Europay, MasterCard and Visa (EMV) chip integrated circuit card and contactless Near Field Communication (NFC) devices. The Contractor shall ensure compliance with EMV chip guidelines for chip card transactions and International Standards Organization (ISO)/International Electrotechnical Commission (IEC) 18092 specifications for contactless NFC transactions.
65	Check scanners (for remote deposit capture) shall include, but not be limited to:
	• high accuracy Magnetic Ink Character Recognition (MICR) rate;
	• compliance with "The Check Clearing Act for the 21st Century" (Check 21);
	• check defacement features and
	• alphanumeric Optical Character Recognition (OCR) A & B font recognition.

1.1.1.8. Network, Communications,Telephony, Security and Surveillance

66	The Contractor shall provide all required network Equipment and communications lines (including all installation and recurring costs throughout the Term of the Agreement) to connect the CSC and BOS to all required users and systems with sufficient bandwidth to meet all Requirements at no additional cost to the Authority, including:
	• secure dedicated and redundant Interface connections for all BOS to CSC personnel communications;
	• remote Contractor personnel;
	• work-at-home Contractor personnel (under certain Business Continuity procedures);
	• secure dedicated and redundant Interface connections for all Contractor designated Third-Party Service Providers;
	• all Contractor provided BOS environments;
	• secure dedicated and redundant Interface connections for customers accessing the BOS or CSC via telephony, IVR, Self-Service Website, Self-Service Mobile Application (Phase II and optional) and all other channels;
	• secure dedicated and redundant Interface connection to ETTM System at 4301 W. MacArthur Blvd, Santa Ana, CA 92794;
	• secure dedicated and redundant Interface connections for the OCTA Store WIC location at 600 S Main St, Orange, CA 92868 via secure public VPN (or other Authority Approved Interface). OCTA will provide all necessary Equipment at the OCTA Store WIC location;

	• secure dedicated and redundant Interface connections for Authority's staff locations from various locations via secure public VPN (or other Authority Approved Interface). OCTA will provide all necessary Equipment at the Authority staff locations and
	• secure dedicated and redundant Interface connections for all Authority designated Third-Party Service Providers via secure public VPN (or other Authority Approved Interface). OCTA or others will provide all necessary Equipment at the Third-Party Service Providers locations.
67	The Contractor shall provide the telephony systems for all CSC Operations personnel at the CSC and the collocated WIC. Note: The telephony system at the OCTA Store WIC at 600 S Main St, Orange, CA 92868 will continue to be provided by OCTA.
68	As part of the Implementation Phase, the Contractor shall provide and install all network Equipment and communications as required to meet the Requirements.
69	The Contractor will assume Maintenance, administration and Upgrade of all network Equipment and communications to service the BOS and CSC throughout the Operations and Maintenance Phase.
70	The network connection to the ETTM System shall be of sufficient bandwidth to support the transfer of images, transactions/trips, Transponder Status Lists and other required files.
71	The Contractor shall increase throughput and bandwidth as needed to eliminate system latency and meet the Requirements.
72	The Contractor shall provide network monitoring Software to monitor all Contractor provided and Authority provided infrastructure, network Equipment and communications related to the BOS and CSC. All network notifications and alarms shall be reported to the PMMS.
73	The Contractor shall provide the capability for time synchronization to one or more certified time server(s). The Contractor shall provide for redundant certified time sources should the primary source be unavailable.
74	The Contractor shall ensure exact synchronization with the ETTM System.
75	The Contractor shall provide secure remote access to the full capabilities of the BOS for Authority Authorized Users working remotely.
76	The Contractor shall be responsible for ensuring that all BOS networks and communications are compliant with the Security Standards.

1.1.2. BOS Functionality

The BOS functionality Requirements begin with the design of a GUI to the BOS. Through the GUI, Authorized Users (from within the CSC) and customers (accessing via the Self-Service Website, and Self-Service Mobile Application (Phase II and optional))) will access a user account and other information within the BOS. This section of the global Requirements also includes Requirements for establishing and controlling user access to the BOS, logging and security controls and maintaining

efficient databases through regular purging and archiving of stale records in accordance with the Security Standards.

1.1.2.1. Graphical User Interface (GUI)

The GUI design must include accepted computer industry design standards for ease of readability, understanding and appropriate use of menu-driven operations, user customization and intuitive operation. The GUI should allow for efficient action by CSR or customer minimizing screens and clicks to modify.

77	The Contractor shall provide a secure, browser-based GUI for the BOS application, Self-Service Website, and all external Interfaces.
78	The Contractor shall provide for secure communications with the BOS application, all customer portals and all external Interfaces, such as Hypertext Transfer Protocol Secure (HTTPS) or similar.
79	The GUI shall adhere to accepted development standards and specifications, including but not limited to World Wide Web Consortium (W3C) and HyperText Markup Language (HTML) Version 5 or current standard.
80	The Contractor shall follow Payment Card Industry Data Security Standard (PCI DSS) and standard security practices in the design of the GUI for the BOS application, all customer portals and all external Interfaces.
81	The GUI design and development shall incorporate human factors and usability engineering and be optimized for speed, as well as provide the following controls, including but not limited to:
	• menus (such as pull down, popup, cascading, leveling, etc.);
	• allowing for multiple windows within the application, such as to navigate back without having to re-enter a user account;
	• informational messages;
	• positive feedback;
	• exception handling and error dialogs, including logging the error (in the PMMS);
	• control icons, links and action buttons;
	• data entry fields, combo boxes, check boxes;
	• display (read-only) fields and
	• general and context-specific help menus.
82	Data entry screens shall have Configurable mandatory fields that require data entry prior to continuing through the process.
83	The Contractor shall provide field-level validation and format verification upon existing data fields applicable to pre-defined formats or standards, including but not limited to:

	• alpha-numeric;
	• date;
	• time;
	• special characters;
	• length;
	• license plate number (based on individual issuing Jurisdiction rules) fields;
	• transponder numbers;
	• telephone number;
	• email address;
	• ZIP or postal codes and
	• check-digit, checksum, Modulus-10 or other verification algorithms for fields such as Credit Card number.
84	The Contractor shall provide field-level "tooltips" or other interactive help, Configurable by the system administrator, that provide specific guidance on any field presented, including but not limited to:
	• alpha-numeric fields;
	• date fields;
	• time fields;
	• special characters;
	• username and password;
	• length restrictions;
	• license plate number (based on individual issuing Jurisdiction rules) fields;
	• transponder fields;
	• telephone number fields;
	• email address fields;
	• ZIP or postal code fields and
	• Credit Card number fields.
85	The Contractor shall provide the capability for Authorized Users to maintain drop-down lists, including but not limited to:
	• add items;

	• deactivate items;
	• set effective activate and deactivate times;
	• modify items;
	• toggle item visibility on/off;
	• set the display order;
	• change the display order;
	• set the default value and
	• change the default value.

1.1.2.2. BOS Application Requirements

86	The Contractor shall provide navigation optimized for speed and with identical screen presentation and user experience, regardless of the browser used. The BOS application shall detect and advise if the browser being used is out-of-date or not supported, as well as instruct where updates can be obtained.
87	Help menu/dialogue box shall be provided for each screen, each editable field and each selectable option within each screen.
88	The Contractor shall provide workflow and application help menus that integrate seamlessly into the user interface.
89	The Contractor shall provide help menus that provide clear descriptions and walk-through procedures for all standard tasks.

1.1.2.3. User Accounts, User-Roles, User-Role Management and Controls

User account management and role management is an important component to the overall security of the solution. Authorized Users are Approved users that have role-based credentials to access the BOS as an employee of the Contractor, employee of the Authority, Third Party Service Provider, or contractor of the Authority.

90	Authorized Users shall access the BOS using an authenticated, role-based login and be uniquely identified and authenticated using a strong password policy.
91	The Contractor shall provide the capability for only privileged accounts to use tools with administrative capabilities conforming to the concept of least privilege.
92	Allow for full integration with Microsoft Active Directory (AD) or similar access system Approved by the Authority so users are not required to enter separate passwords for system access (the BOS shall prompt users for their credentials and not allow pass-through authentication), and that all rules for password security (for example, characters or rotations) are enforced and passed between the network and the application.
93	The Contractor shall provide the capability to create (Configurable) BOS user accounts.

94	The Contractor shall provide the capability to create a new user account having the same role/rights as an existing user account.
95	The Contractor shall provide the capability to allow first name, middle name and/or last name to be changed without having to create a new user account, such as to correct an error or make a change because of marriage or divorce.
96	The Contractor shall provide the capability to search for Authorized Users using Configurable criteria.
97	The Contractor shall provide the capability to track user accounts created dates and disabled dates information, since user accounts may be enabled and disabled repeatedly over a period of time (because of leaves of absence, etc.).
98	The Contractor shall provide the capability to search and view all information about a user account on a particular date and time.
99	The Contractor shall provide the capability to control all access rights within the BOS through the assignment of user-roles.
100	The BOS shall prevent the direct assignment of rights to an Authorized User, and all rights must flow from a user-role.
101	The Contractor shall provide the following user-role capabilities, including but not be limited to:
	• allow Authorized Users to belong to multiple user-roles;
	• allow the deactivation of a user-role, provided no active Authorized Users are assigned to that role;
	• ensure modifications to roles are immediately propagated through the BOS and to all Authorized Users currently assigned to the role;
	• prevent BOS access to users who are not assigned to a user-role and
	• provide a built-in “read-only” capability that can be added to any user-role, allowing user accounts assigned to that role to view information on the screen and print reports (but not make changes).
102	The Contractor shall provide the capability for an Authorized User to view the summary of permissions of a user created with multiple user-roles.
103	The Contractor shall provide the capability for Authorized Users to manage user-roles, including but not limited to:
	• create new user-roles;
	• change access rights;
	• assign and un-assign user-roles to user accounts;
	• assign and un-assign user accounts to user-roles;

	• adjust user-roles and
	• deactivate user-roles.
104	The Contractor shall provide the capability for Authorized Users to manage multiple levels of access control based on user-roles, including but not limited to:
	• broad functional level, for example, user-role X is denied access to the user account management functionality;
	• detailed functional level, for example, user-role Y is allowed access to the user account management functionality but denied access to close user accounts function and
	• field level, for example, user-role Z is allowed access to the user account management functionality but denied access to the tax-exempt checkbox.
105	The Contractor shall provide the capability for Authorized Users to deny/allow access or allow read-only access, based on user-roles, including but not be limited to:
	• specific menus;
	• specific items on a drop-down list;
	• specific individual screens;
	• specific functions on a screen;
	• specific fields within a specific screen;
	• specific types of transactions/trips;
	• specific processes;
	• specific reports;
	• specific activities based on account status;
	• specific search capabilities;
	• specific transaction/trip approval privileges;
	• specific workstation location access;
	• specific workstation time restrictions and
	• specific time restrictions.
106	The Contractor shall provide the capability to configure Flags as part of a user role definition, so they can be viewed based on user-roles.
107	The Contractor shall provide the capability to send Alerts to the PMMS for logging and notification based on the assignment/removal of a specific user-role (Configurable as new user-roles are created).

108	The Contractor shall provide the capability to search for all Authorized Users with a specific role and all user accounts with a specific access right.
109	The Contractor shall provide the capability to search and report on user-roles for a particular date, distinguishing between an active user account (able to access information according to its roles) an inactive user account (temporarily unable to access information because of a locked password or expired from lack of use) and a disabled user account (a user account no longer able to access information because of the intervention of an Authorized User).
110	The BOS shall keep a full history of all user-role details with effective dates so the exact rights for a particular user-role can be viewed by Authorized Users at any point in time.

1.1.2.4. Logging Mechanisms

These mechanisms provide chronological recording of system events and user account activities. They also document the sequence of activities that have been affected at any time during a specific operation, procedure or event.

111	The Contractor shall provide comprehensive, system-wide logging capabilities ensuring every change to a BOS record of any type is logged with a date/time stamp, including the Authorized User (and IP address) that made the change.
112	The Contractor shall ensure that system clocks are synchronized. For example, Desktop Environments, Equipment, servers, physical security systems and CSC Surveillance CCTV systems.
113	The Contractor shall provide the capability to log all changes to user accounts.
114	The Contractor shall provide the capability to log all changes to the Processing Exception List.
115	The Contractor shall provide BOS reports, including but not limited to:
	• reports of logged activity by activity type and
	• reports of logged activity by user accounts.
116	The Contractor shall create a log when a user-role is assigned, changed or removed from a user account.
117	The Contractor shall provide screens so Authorized Users can view all log files.
118	The Contractor shall provide the capability to log and track all user activities and user accounts viewed by specific user account with date, time stamp, and workstation location.
119	The Contractor shall provide Configurable Alerts to the PMMS for all functions of the BOS which are logged.
120	The Contractor shall provide logging that includes actions taken within a user account with date and time stamp.

121	The Contractor shall provide logging of all changes (view, add, delete, modify) to Credit Card information.
122	The Contractor shall provide logging of all user login attempts, including but not limited to:
	• username;
	• originating Internet Protocol (IP) address;
	• date;
	• time and
	• success/failure.
123	The Contractor shall provide logging of all customer login attempts, including but not limited to:
	• Uniform Resource Locator (URL);
	• user account;
	• browser/platform including version number;
	• originating IP address;
	• date;
	• time and
	• success/failure.
124	The Contractor shall provide audit logging capabilities that provides the ability for view access by CSR and/or by account to have the review of users that have accessed the account or Case even if no changes have been logged.
125	The Contractor shall create a log of all changes to system configurations or settings and record the user name, date, time and IP address from which the change was made.
126	The Contractor shall be in compliance with all PCI DSS logging requirements while preventing any logging of Credit Card numbers or card verification value data, including debugging and error logs.
127	The Contractor shall be in compliance with all PII logging requirements while preventing any logging of PII data, including in debugging and error logs.
128	The Contractor shall provide the capability to generate an Alert to the PMMS when debugging logs are turned on within the production environment.
129	The Contractor shall prevent tampering with log file data.
130	The Contractor shall provide the capability to log and track changes to applications, databases and operating systems.

1.1.2.5. BOS Security Standards, PCI-DSS, PII and Best Practices

The Contractor shall provide security and access controls in accordance with the Security Standards. These Security Standards will evolve as standards, best practices and California statutes evolve over the Term of the Agreement.

131	The Contractor's approach to BOS and user security shall continually provide adherence to the latest specifications, publications, policies and standards, including but not be limited to:
	• compliance with PCI DSS;
	• protecting the confidentiality of PII in accordance with the Authority's privacy policy;
	• protecting the confidentiality of PII in accordance with Section 31490 of the Streets and Highways Code and other applicable California statutes;
	• protecting the confidentiality of PII in accordance with the recommendations in publication 800-122 from the National Institute of Standards and Technology (NIST) or subsequent versions;
	• protecting the confidentiality of PII in accordance with California Consumer Privacy Act (CCPA);
	• protecting the confidentiality of PII in accordance with California Online Privacy Protection Act (CalOPPA);
	• encryption of data in accordance with NIST SP 800-111 Guide to Storage Encryption Technologies for End User Devices;
	• protecting the confidentiality of PII in accordance with the California Civil Code Section 1747.08.;
	• account for information security management risk as described by NIST Cybersecurity Framework special publication 800-39;
	• conformance to applicable best practices for information security management as described by the ISO/IEC 27000 standards;
	• the security Requirements and
	• all California and out-of-state DMV security requirements and standards.
132	The Contractor shall Design the System to anticipate that during the Implementation and/or Maintenance Phases the System will become subject to more restrictive digital privacy laws and regulations (for example, similar to European Union General Data Protection Regulation (GDPR)). During Design within the Implementation Phase, the Contractor shall provide documentation (within applicable deliverables) and demonstrate (during testing) the System's preparedness to anticipate more restrictive privacy Requirements.

133	The Contractor shall establish and maintain a formal, documented, mandated, BOS and CSC Operations information security policy that shall be communicated to all Contractor and Subcontractors personnel in a relevant, accessible, and understandable form and will be regularly reviewed and evaluated to ensure its operational effectiveness, compliance with all Security Standards, applicable laws and regulations, and to address new threats and risks.
134	The information security policy shall address all removable media except in the context of Contractor's routine back-ups or as otherwise specifically Approved by the Authority, Contractor shall institute strict physical and logical security controls to prevent transfer of BOS data via removable media.
135	The Contractor shall provide strong end-to-end encryption for all sensitive information, including PCI and PII) stored within databases (at rest) or being transmitted (in-motion).
136	The Contractor shall use strong encryption methods such as AES FIPS-179 (128 bits and higher) or RSA (2048 bits and higher), or an equivalent if Approved by the Authority.
137	The Contractor shall provide encryption keys that are considered sensitive information and stored on appropriately secured servers.
138	The Contractor shall prevent any unauthorized user, system or database administrator from viewing encrypted information in unencrypted form, while providing the capability for Authorized Users to view encrypted information in unencrypted form to perform tasks based on a defined role.
139	The Contractor shall ensure that no cardholder data, such as Credit Card numbers or card verification value data, is in any BOS environments.
140	The Contractor shall ensure that no PII data is in the BOS environments other than production, DR and test.
141	The Contractor shall provide comprehensive user credential controls that are compliant with PCI standards, including but not limited to:
	• prevent the creation of 'generic' user accounts – all user accounts shall be associated to a specific person. For example, use the unique employee ID as a required field for each user account. Duplicate IDs would be rejected and
	• prevent a user (role-based) from logging in at two different machines at the same time, while allowing a single user on a single machine to have multiple sessions open at the same time.
142	The Contractor shall provide the capability to configure different user credential controls for different types of users, including but not limited to:
	• Authorized Users who will access the BOS;
	• Third-Party Service Providers that access the BOS via external Interfaces and
	• customers who will access the BOS via the Self-Service Website, Self-Service Mobile Application (Phase II and optional) and the IVR.

143	All Hardware shall be integrated with the PMMS and configured to provide PMMS alerts in relations to out-of-date security software and patch versions.
144	All Hardware shall be integrated with the PMMS and configured to provide PMMS alerts in relations to all attempted intrusions, virus attacks, ransomware attacks, spamming, denial of service and attempted/successful unauthorized access.
145	For any Hardware removed from the BOS, the Contractor shall provide a notarized statement, detailing the removal or destruction method used, the data sets involved, the date of destruction, and the company or individual who performed the destruction. The statement shall be sent to the Authority within fifteen (15) Calendar Days of removal of the Hardware. The destruction or erasure of data or information pursuant to this section shall be in compliance with industry Best Practices (e.g., NIST SP 800-88, Guidelines for Media Sanitization)
146	The Contractor shall provide a report of all security incidents. The Authority or its third-party designee may, but is not obligated to, perform audits, security tests and intrusion tests of BOS environments that may also include, but are not limited to, interviews of relevant personnel, review of documentation, and/or technical inspection of systems.
147	The Contractor shall provide for Authority's review any original security reports related to security assessments that the Contractor has undertaken to assess BOS and shall notify the Authority of all security assessments.

1.1.2.6. Archival and Purge Control Mechanisms

The Authority is public and, therefore, are subject to the law governing the retention and disposition of information considered as public record. The Requirements for archiving and purging include Requirements for automating these activities in a way that maintains compliance with the Contractor retention schedule that is provided as part of the Contractor's Maintenance documentation, while providing the Authority a method to Approve the disposition of records before they are deleted.

148	The Contractors archival and purge processes shall be in compliance with the data retention Requirements set forth in the Security Standards and Volume I, Section 4.2.17 Records.
149	The Contractor shall provide the capability for fully automated and Configurable storage of historical data (archival) and the permanent deletion of inactive or obsolete data (purging).
150	The Contractor shall provide the capability to store 100 percent of the BOS electronic information in accordance with the data retention Requirements set forth in the Security Standards and Volume I, Section 4.2.17 Records.
151	The Contractor shall provide the capability to store 100 percent of the BOS electronic historical information indefinitely if they have enduring significance to the Authority's activity (i.e., permanent, evidentiary, and/or historical value) in accordance with the retention schedule. All information, other than that prohibited within the Requirements, will be retained for the duration of the Agreement and archived or moved to long-term storage as deemed appropriate during the Implementation Phase to meet all customer and Authority needs for reporting and data access

152	Archival and purge routines shall be Configurable for each impacted data element, including but not limited to:
	• transactional data;
	• all formats of customer PII data;
	• Images (Violations-related and I-Toll-related);
	• documents;
	• Notifications;
	• BOS logs and
	• third-party provided files.
153	The Contractor shall provide the capability to archive data on a monthly interval.
154	The Contractor shall provide the capability to purge archived data on a periodic basis.
155	Authorized Users shall have the capability to request retrieval of archived data through the Contractor's ticketing system included in the PMMS.
156	All archived data shall be stored on permanent, long-term storage media and shall be maintained at a secure Authority Approved third-party commercial data storage facility.
157	Servers shall retain transaction/trip and summarized data, all images and BOS logs online for a specified period of time and then archive that data.
158	Data shall be purged in accordance with the data retention schedule.
159	The Contractor shall provide the capability to notify the BOS Maintenance personnel via the PMMS a Configurable number of days in advance and require Authorized User approval for when archival and purging jobs are to be executed, including but not limited to data elements impacted, date range applied and data size impact.
160	After successful archival of data and confirmation via the PMMS, the deletion of online data shall be automatic, without user intervention and shall generate a message to be transmitted according to the PMMS rules. Absolutely no transactions/trips shall be deleted unless confirmed to be successfully archived.
161	The BOS servers shall be sized to accommodate for the restoration of selected archived data (one -year minimum).
162	Authorized Users shall be able to generate queries from the restored data.

1.1.3. Interfaces

The Contractor is responsible for working with the Authority, Interoperable Agencies/California Toll Operators Committee (CTOC) and Third-party Service Providers in designing, developing, documenting, testing and implementing all required Interfaces and portals.

1.1.3.1. General Requirements for External Interfaces

Electronic Interfaces are required to provide BOS connectivity. The technical specifications for these Interfaces are documented in ICDs that have either already been developed by the Authority or shall be developed by the Contractor. The ICDs include Requirements for data format and transmission, criteria for acknowledgement and validation of transmitted data and procedures for recording and reconciliation as appropriate for each Interface.

163	The Contractor shall develop new or comply with existing electronic Interfaces at the direction of the Authority.
164	The Contractor shall provide for guaranteed transmission of data for all Interfaces and portals.
165	The Contractor shall provide for 100 percent reconciliation of the transmitted and received data and files.
166	The Contractor shall provide the capability for Authorized Users to access and view the contents of files, including compressed or encrypted files, which are received by the BOS and transmitted by the BOS in a readable format. Authorized Users shall have the capability to save the contents of such files.
167	The Contractor shall provide the capability for sending real-time Alerts to the PMMS for Interface and data transmission failures, including but not limited to:
	• real-time dashboard for managing and monitoring Interfaces;
	• workflow user Interface for managing and monitoring steps within each Interface;
	• status and history of executions;
	• comprehensive scheduling of file transmissions;
	• tools for viewing data and/or contents of files received via Interfaces and portals (compressed or encrypted);
	• comprehensive reporting for transmitted and received data and files;
	• tight integration with the PMMS and notification of failed transmissions and
	• capability to manually execute a failed transmission.
168	When using File Transmission Protocol (FTP), the Contractor shall utilize Secure File Transmission Protocols (SFTP) for the transfer of data and/or files via Interfaces and portals.
169	The Contractor shall provide the capability to transmit and receive multiple files during each scheduled batch.
170	The Contractor shall provide the capability to transmit and receive multiple full and incremental files in a day.

171	The Contractor shall utilize file naming conventions that prevent the over-write of data and/or files. For example, include the date and time of transmission.
172	The Contractor shall provide file handling and processing methods that provide for a complete log of the data and/or file transfer process.
173	The Contractor shall validate records and identify errors in the received data and/or files, including but not limited to:
	• mandatory fields;
	• data formats;
	• data validity (for example, user account number not found in the BOS);
	• duplicate records;
	• unexpected response;
	• checksum/record count verification and
	• incorrect status.
174	The Contractor shall provide the capability to correct and re-transmit data and/or files (the process shall be automated to the extent possible).
175	The Contractor shall provide the capability to process re-transmitted data and/or files.
176	The Contractor shall provide the capability to transmit the error details to the transmitting entity, as well as record it in the PMMS.
177	The Contractor shall provide the ability to identify missing records/transactions/images and request the transmission of such missing records/transactions/images.
178	The Contractor shall reconcile the transmitted records to the records received and accepted by the receiving entity.
179	The Contractor shall provide the means to identify Interface issues by validating the file transmission process, including but not limited to:
	• creation and transmission of data and/or a file at the scheduled time, even if there are no records to transmit;
	• determination if the data and/or a file was transmitted or received at the scheduled time;
	• creation of Alerts to the PMMS if data and/or a file was not created or received at the scheduled time;
	• creation of Alerts to the PMMS if received data and/or a file was not acknowledged;
	• creation of Alerts to the PMMS if records in the received data and/or file had errors when processed;

	• provide details in real-time to the PMMS of each failed record and
	• creation of Alerts to the PMMS when a response has not been received for individual records within the expected duration.
180	The Contractor shall provide data and/or file transmission and reconciliation reports as described in these Requirements.
181	All responses received from third-party Interfaces and all actions required of the third-party to a file transmitted by the BOS shall be associated with the original transaction, including but not limited to:
	• Violation data and images;
	• images of check copies for a payment;
	• Notifications to customers transmitted by the Collection Agency;
	• comments and dispositions transmitted in the response file and
	• emails received from the customer related to a specific transaction/trip or Violation.
182	The Contractor shall provide the capability for Authorized Users to obtain the history of updates to a transaction/trip.
183	The Contractor shall provide a dashboard that tracks the progress of data and/or file transmissions through each stage and their acknowledgements by the receiving entity, including but not limited to:
	• transactions/trips eligible for transmission;
	• file and/or data created with file name;
	• file and/or data transmitted;
	• file and/or data received;
	• file and/or data accepted;
	• file and /or data rejected;
	• file and/or data re-transmitted;
	• number of records in the file and/or data set;
	• number of unique user accounts and
	• number of failed records.
184	The Contractor shall provide the capability for Authorized Users to configure the relevant parameters related to file and/or data transmission for each Interface. For example, scheduling the time-of-day that a specific file is transmitted.

185	The Contractor shall monitor the disk capacity where files and/or data are deposited and send an Alert to the PMMS and third-party entities (if applicable) if folders are near capacity (Configurable) or full.
186	The Contractor shall provide the capability to automatically archive successfully processed data and/or files after a number of days (Configurable).
187	The Contractor shall provide the data to reconcile file transmissions.
188	The Contractor shall conform to any existing ICDs, including any updates required at the time of design and develop all new ICDs that are required to be developed. It is the Contractor's responsibility to ensure all ICDs (including existing) are accurate, updated and meet the Requirements of the BOS before developing the Interfaces. Standards-based Interfaces shall be used when available and all Interfaces shall be Approved by the Authority.
189	Where the Third-party Service Provider currently supports or is willing to develop a more modern and current interface, the Contractor shall be responsible for developing the ICD or using the ICD to develop the new Interface as directed by the Authority.
190	The Contractor shall implement required updates to Interfaces at the direction of the Agencies at no additional cost to the Agencies.

1.1.3.2. Interface to the ETTM System

This Interface connects the BOS with the ETTM System for transmitting transactions/trips, images, toll rate information, transponder files, license plate files and other data to the BOS for processing and for transmitting various data back to the ETTM System.

191	It is anticipated that the BOS shall receive, process and store an average of four (4) transactions per trip, including both Toll Collection Enforcement Site (TCES) and Toll Transponder Read Site (TTRS) transactions.
192	If the BOS implementation requires an update to the ETTM System ICDs, the Contractor shall develop the new ICD and coordinate all design, development and testing with the ETTM System Contractor.
193	The ETTM System ICDs may include many data fields, including but not limited to:
	• trip transaction ID;
	• trip ID;
	• timestamp for when the trip started;
	• amount of time that was being allotted for travel from the pricing sign to the Toll Zone;
	• Occupancy Setting applied for the overall trip;
	• Clean Air Vehicle identifier for overall trip;

	• motorcycle identifier for overall trip;
	• image-based or a tag-based trip identifier;
	• total toll rate assigned for the trip;
	• total toll rate that was in effect at the time of the trip;
	• primary transponder ID for the overall trip;
	• license plate number for the overall trip;
	• Jurisdiction of the license plate for the overall trip;
	• license Plate Type for the overall trip;
	• segment identifier;
	• lane identifier;
	• lane mode identifier;
	• Straddle – This is a yes/no type identifier for whether the vehicle was straddling the lane line when it went through the Toll Zone;
	• timestamp for when the transaction occurred;
	• transponder items below shall be enumerated for each transponder read at the Toll Zone, with all of the subsections being listed for each transponder;
	• transponder ID;
	• timestamp when the transponder was read;
	• transponder status;
	• transponder type;
	• transponder Occupancy Setting;
	• primary transponder identifier;
	• buffered transponder read identifier;
	• spurious transponder read identifier;
	• license plate number selected for the transaction based on confidence values;
	• Jurisdiction of the license plate selected for the transaction based on confidence values;
	• license Plate Type selected for the transaction based on confidence values;
	• OCR confidence;

	• Occupancy Detection System occupancy assigned (if applicable);
	• occupancy assigned;
	• Clean Air Vehicle identifier;
	• motorcycle identifier;
	• vehicle classification;
	• Image items below shall be enumerated for each image captured at the Toll Zone, with all of the subsections being listed for each image;
	• file name for the image;
	• camera that took the image;
	• timestamp for when the image was captured;
	• license plate number reported by the OCR/image review system for the individual image;
	• Jurisdiction of the license plate reported by the OCR/image review system for the individual image;
	• license Plate Type reported by the OCR/image review system for the individual image;
	• OCR confidence value for the license plate assigned by the OCR/image review system for the individual image and
	• payment type identifies whether the individual transaction registered as an Image-Based or a Transponder-Based Transaction.
194	The Contractor shall Interface to the ETTM System to obtain and acknowledge 100 percent of all transactions/trips, associated transaction and Violation images in accordance with the ICDs to be developed during Project design.
195	The ETTM System Interface shall be capable of the following Configurable functionality, including but not limited to:
	• sending the comprehensive and incremental Authority Tag Status Files and License Plate Status Files (for both the CTOC Agencies' and Interoperable Agencies') in real-time and at scheduled intervals (e.g., every 10 minutes). The BOS shall support sending the Tag Status File and Plate Status File as single file or as separate files;
	• sending Interoperable Agency transponder statuses periodically (incremental and comprehensive) multiple times per day (e.g., every 10 minutes);
	• sending rental car files (incremental and comprehensive) multiple times per day (e.g., every 10 minutes);

	• sending Plate Correction List from customer disputes and audit checks no less than every hour;
	• sending Processing Exception List maintained at the BOS no less than every hour;
	• receiving Transponder-Based Transactions/Trips;
	• receiving Image-Based Transactions/Trips (including license plate number, Jurisdiction, and type, if required) and
	• receiving other files (such as toll rate schedules and variable pricing information).
196	The Contractor shall provide the capability to positively acknowledge (ACK) message receipt, negatively acknowledge or reject a message (NACK) and reconcile data transmissions from the ETTM System.
197	The Contractor shall receive and store color and black and white images for each transaction that comprises the trip, from the ETTM System including:
	• ROI image(s) – average of approximately 8KB per image;
	• full rear image(s) – average of approximately 450KB per image;
	• full rear straddle image(s) – average of approximately 450KB per image and
	• overview image(s) – average of approximately 450KB per image.

1.1.3.3. Interface to the Interoperable Agencies

This Interface connects the BOS with the Interoperable Agencies for data exchange.

198	The Contractor shall provide the Interface to WRTO/CTOC Interoperable Agencies and Regional and National Hubs, for the functionality described within these Requirements and in accordance with latest and future WRTO/CTOC ICDs. The Contractor shall support Interoperable agencies that will be on different versions of the WRTO/CTOC ICD throughout the Term of the Agreement.
199	The Contractor shall provide the capability to obtain and acknowledge 100 percent of all transactions/trips and images from Interoperable Agencies.
200	The Contractor shall provide the capability to transmit 100 percent of all Interoperable Agency customer transactions/trips and images to their respective Interoperable Agencies.
201	The Contractor shall provide the capability (Configurable) to transmit the Authority's plaza update (including addition of new plaza facilities) information to Interoperable Agencies.
202	The Contractor shall provide the capability (Configurable) to receive Interoperable Agencies' plaza update (including addition of new plaza facilities) information.
203	The Contractor shall provide the capability (Configurable) to transmit the Authority's Transponder Status Lists (TSLs) to Interoperable Agencies.

204	The Contractor shall provide the capability (Configurable) to receive Interoperable Agency TSLs from Interoperable Agencies.
205	The Contractor shall provide the capability (Configurable) to transmit BOS customer license plate numbers to Interoperable Agencies.
206	The Contractor shall provide the capability (Configurable) to receive license plate numbers from Interoperable Agencies.

1.1.3.4. Interface to California and Arizona DMV

This Interface connects to the California, Arizona, Oregon and Nevada DMVs to obtain information (such as name, address, vehicle make/model, CAV designation, VIN) about vehicles which fail to properly pay the toll amount.

207	The Contractor shall provide and administer a direct DMV Interfaces for the purpose of obtaining for vehicles travelling in the Express Lanes Facility and the placement and release of vehicle Registration Holds, including.
	• California DMV;
	• California Temporary License Plate DMV database;
	• Arizona DMV (including Temporary License Plate DMV database if applicable);
	• Oregon DMV (including Temporary License Plate DMV database if applicable) and
	• Nevada DMV (including Temporary License Plate DMV database if applicable).
208	Whenever available, the Contractor shall use the on-line DMV Interface allowing for real time look ups and updates. If multiple DMV Interfaces are available to provide the same information, during the Implementation Phase the Authority shall direct the Contractor as to which Interface to implement.
209	The Contractor shall obtain approval from all DMVs to be a processor for the Authority.
210	The Contractor shall maintain all security requirements required by all DMVs.

1.1.3.5. Interface to Rental Car Service Providers

This Interface connects to Rental Car Service Providers to exchange transactions/trips, vehicle, renter information, rental agreements and payment information with the BOS, for rental cars that incur tolls on the Authority's Toll Facilities.

211	The Contractor shall provide the capability to transmit and receive vehicle information from all rental car companies using a Rental Car Service Providers.
212	The Contractor shall provide the Interfaces to Rental Car Service Providers for the functionality described within these Requirements and in accordance with ICDs to be developed during Project design.

213	The Contractor shall provide the capability to schedule and automatically send periodic (Configurable) detailed rental car account toll transaction/trip files to Rental Car Service Providers.

1.1.3.6. Interface to Tranporation Corridor Agencies (TCA) for the Dispostion of Rental Car Trips

The Transportation Corridor Agencies (TCA) intends to host rental car plates and transponders and collect tolls on behalf of other CTOC agencies.

214	The Contractor shall provide the capability to transmit and receive vehicle information from TCA in a separate TSL and License Plate Status File IOP file.
215	The Contractor shall provide the capability to provide TCA with toll amounts due for the plates and transponders in the rental file and process payments from TCA.

1.1.3.7. Interface to the Authority's BOS Bank

This Interface is to the Authority -provided bank to retrieve all required banking information.

216	The Contractor shall provide an Interface to the Authority Bank to retrieve, process and store all information required to support the all-electronic BOS bank reconciliation process.
217	The Interface shall support the use of Positive Pay to deter check fraud.

1.1.3.8. Interface to California Franchise Tax Board (FTB) Tax Intercept Program

This Interface is to the California FTB Tax Intercept Program to provide and receive all required Tax Intercept information.

218	The Contractor shall provide an Interface to the California FTB to retrieve, process and store all information required to support the Tax Intercept process.

1.1.3.9. Interfaces to Authority's Financial Accounting Systems

219	The Contractor shall provide an Interface to the Authority's financial accounting system for the purpose of issuing accounts payable checks.
220	The Contractor shall provide an Interface to the Authority's financial accounting system for the purpose of recording financial activity to the general ledger.

1.1.3.10. Interface/Connectivity to Contractor-Provided Services

The Contractor shall provide connectivity to service providers for which the Contractor is responsible. The Requirements are not prescriptive as to the Interface type or method.

221	The Contractor shall provide connectivity to Contractor selected Third-party Service Providers as required to meet the Requirements, including but not limited to:

	• Collection Agency 1 (Direct Access to BOS is Phase II Functionality);
	• Collection Agency 2 (Direct Access to BOS is Phase II Functionality);
	• Customer Satisfaction Survey Provider Subcontractor;
	• Lockbox Service Provider (optional);
	• Merchant Service Provider 1;
	• Merchant Service Provider 2;
	• 3rd Party ROV Lookup for all 50 states (excluding direct connect DMVs), District of Columbia, U.S. Government and
	• Print/Mail House Service Provider (optional).

1.1.4. Performance Management and Monitoring System

The Performance Management and Monitoring System (PMMS) supports BOS Maintenance Requirements for all Hardware, Software and other BOS components by monitoring BOS processes, Equipment, jobs and Interfaces in real-time to identify degradations in performance or availability before they impact end users. The PMMS generates Alerts and creates actionable trouble tickets that can be tracked to resolution.

222	The Contractor shall provide a PMMS that supports BOS Maintenance Requirements for all Hardware, Software and other BOS components, in accordance with these Requirements.
223	The Contractor shall provide a PMMS that monitors, Alerts and generates trouble tickets in real-time for all BOS processes, Equipment, jobs and Interfaces, including but not limited to:
	• communications issues;
	• electrical power issues;
	• temperature issues;
	• Hardware issues;
	• Software issues or failures;
	• database issues;
	• anomalies to the system design;
	• issues with customer portals (Self-Service Website and Self-Service Mobile Application (Phase II and optional));
	• file systems and file system issues;
	• issues with jobs, processes or data flows;
	• BOS health – overall and by component;

	• BOS and application performance;
	• BOS utilization – disk space, disk IOs, CPU, memory, throughput (Configurable thresholds);
	• security events;
	• Logs;
	• access controls;
	• CSC CCTV Surveillance System and
	• CSC physical security systems.
224	The PMMS shall provide comprehensive recording capabilities, including but not limited to:
	• log aggregation (from disparate systems or Modules);
	• event correlation (cause and effect association);
	• log shipping and
	• log management functions.
225	The PMMS shall have the ability to receive success or failure information regarding data management activities, including but not limited to:
	• backup;
	• DR data transfer and synchronization status;
	• data archival and
	• data restores.
226	The Contractor shall provide a PMMS that monitors, alerts and tracks, in real-time, unusual or potentially fraudulent activity triggered by users and systems, including but not limited to:
	• multiple one-time replenishments coupled with closing of customer accounts;
	• repeated opening and closing of customer accounts;
	• refunds over a dollar amount (Configurable) and
	• multiple deposits and refunds on the same customer account.
227	The PMMS shall monitor that all BOS components have current and up-to-date virus, firewall and spam protection and other security Software that prevent single point of vulnerability from external threats, virus attacks, ransomware, spam protection and unauthorized access.

228	The Contractor shall provide a PMMS that monitors, alerts and tracks, in real-time, unusual or potentially fraudulent activity, including but not limited to:
	• attempted network or system intrusions;
	• attempted malicious attacks and
	• Unexpected changes to security settings on firewalls and other security systems.
229	The PMMS shall include, but not be limited to the following capabilities:
	• receiving and monitoring status messages for all BOS Hardware and Software;
	• grouping, sorting and filtering by message type, time, Equipment, subsystem, etc.;
	• local trouble ticket manual entry or email entry by users;
	• automatic work order generation;
	• storing data in a relational database to allow for data recovery and flexibility in reporting the raw data (including dashboards and ad-hoc reporting);
	• generating (automatically) monthly performance reports;
	• tracking service requests;
	• assigning priorities and actions to events;
	• notifying (automatically) Maintenance personnel via reports, text and email;
	• assigning trouble tickets to Maintenance personnel;
	• reassigning (manually) trouble tickets to other Maintenance personnel;
	• escalating (automatically) trouble tickets to other Maintenance personnel;
	• recording time of acknowledgement by Maintenance personnel;
	• recording time of acknowledgement by all subsequently assigned Maintenance personnel;
	• recording time of repair;
	• recording time of Equipment recovery;
	• recording completion of service calls;
	• attachment of common document type, such as Microsoft Word, Portable Document Format (PDF), email and screen capture images;
	• providing automatic Alerts for trouble tickets not closed in a specified time;
	• maintaining and tracking repair Maintenance activity;

	• calculating response times, repair times and down time from the data entered by the Maintenance staff and automatically generated by the BOS;
	• accepting and updating trouble tickets from mobile hand-held devices and smart phone entries;
	• role-based security;
	• automatic system exception reporting for all processes that are not running;
	• automatic system workflow exception reporting for all items that are not processing correctly or are hung up in the BOS and
	• providing hard copy reports on issues, failures and trouble resolution status.
230	The PMMS shall record all configuration data in a configuration management database, which shall be updated after each system component change, including application of BOS patches.
231	The PMMS shall provide system Maintenance personnel with screens, dashboards and reports within the PMMS that allows for the verification and monitoring of all processes, programs and scheduled tasks. Failures shall be visible in a PMMS screen accessible to Maintenance personnel. Event and error logs shall be provided to assist Maintenance personnel with investigating problems.
232	All PMMS screens, dashboards and reports shall be available to Authorized Users from the Authority.
233	The PMMS shall provide Authorized Users with operational, management and performance reports from the PMMS that include but are not limited to:
	• summarized and detailed alarm history;
	• Maintenance paging and response history;
	• work order status and tracking;
	• Equipment inventory and life cycle tracking;
	• Equipment availability;
	• preventive and predictive Maintenance;
	• corrective Maintenance;
	• response and repair times for each of the priorities;
	• Equipment use history;
	• Equipment repair history;
	• total System availability;

	• sub-System availability for components of the BOS, IVR System, Self-Service Website and Self-Service Mobile Application (Phase II and optional);
	• Equipment versions, Software versions, firmware versions and serial numbers for all Equipment installed under these Requirements;
	• incident logs and lost revenue estimates;
	• performance reports detailing compliance to the Performance Measures;
	• a detailed list of parts replaced as a result of Maintenance actions;
	• status of removed parts and Equipment with an aging status for parts under repair or replacement (serial numbers, being repaired in Maintenance shop, purchase replacement part);
	• performance reports;
	• an exceptions report summarizing all unusual or significant occurrences during the period and
	• trend analysis for repetitive failure.
234	The PMMS shall support the management of preventive/predictive Maintenance schedules.
235	The PMMS shall provide the capability to automatically generate work orders for preventive/predictive Maintenance tasks.
236	The Contractor shall provide a PMMS that supports asset management, including but not limited to:
	• tracking all System Hardware and Software items;
	• tracking all System Hardware and Software locations;
	• tracking all System Hardware and Software versions;
	• tracking all Maintenance and service agreements;
	• maintaining a list of vendors from which products were procured;
	• associating the original purchase order number to the individual item;
	• associating the original vendor to the individual item;
	• associating all warranty information to the individual item and
	• providing an Alert prior to warranty, license, and certification expiration.

1.2. BOS Maintenance and Support Requirements

The Requirements described in this section detail the Contractor's responsibility for providing Maintenance and Software Support Services for the BOS, and associated communications and support to operations, including but not limited to:

- Hardware Maintenance (servers, storage, network switches, firewalls, routers, etc.) if required;
- network administration;
- system administration;
- administration of CSC Facility physical security systems;
- administration of CSC Surveillance CCTV systems at CSC Facility;
- database administration;
- Maintenance and Software Support Services;
- monitoring services;
- on-site desktop and application support services within the I-405 CSC and WIC;
- on-site desktop and I-405 BOS application support services at the OCTA Store WIC (OCTA provided Equipment);
- support of work at home CSRs and operations during Business Continuity;
- application support for the Authority's staff and
- BOS security.

In delivering the Maintenance and Software Support Services, the Contractor is expected to provide the following services, including but not limited to:

- well documented Maintenance schedules and processes;
- change and configuration management;
- on-site support of the BOS;
- complete around-the-clock Maintenance of the BOS;
- significant participation with the Authority's staff, meetings and processes and
- ample spare parts inventory and support agreements.

237	The Contractor shall be responsible for performing all Maintenance activities and fully supporting and maintaining the BOS from Go-Live throughout the Operations and Maintenance Phase.
238	The Contractor shall provide Maintenance, including but not limited to all Equipment, Hardware, Software, cloud-based systems, and systems provided under this Agreement, including Maintenance associated with the compliance with the terms of the Software warranty.
239	The Contractor shall provide Maintenance and Software Support Services, including but not limited to: monitoring; preventive; predictive; corrective, and emergency Maintenance and Software Support Services, as well as any required and planned Upgrades and Enhancements to be performed on any and all BOS elements.

240	To ensure BOS performance is optimized, all system administrative functions, if not otherwise automated, shall be performed at regular, scheduled intervals as part of the preventive Maintenance and Software Support Services in accordance with the Maintenance Plan.
241	The Contractor shall administer, maintain (as required in conjunction with Authority paid Maintenance agreement) and be the point of contact for all Authority provided and paid for Equipment, systems and Maintenance agreements, including uninterruptable power Equipment, power generators, CCTV Surveillance and physical security systems at the I-405 CSC and WIC Facility.
242	The Contractor shall provide on-site Desktop Environment and BOS application technical support to all Contractor personnel and Authority Authorized Users at all locations from 7 a.m. to 7 p.m. Monday – Friday, Pacific Time and be on-call and available to come on-site 24x7x365.
243	The Contractor shall provide support for work-at-home CSRs and operations and in accordance with the Approved Disaster Recovery and Business Continuity Plans. For example, during an event similar to the COVID-19 outbreak.
244	Continuous monitoring of BOS operations shall be performed to verify its functional, processes are being executed as scheduled and that the BOS is operating per Performance Measures. Continuous monitoring shall include but not be limited to:
	• verifying system alarms and Alerts;
	• verifying processes/programs/job have successfully completed as scheduled;
	• evaluating sample transactions data and aggregate data trends for exceptions;
	• confirming trip/transaction and image transmission to and from the ETTM System;
	• performing routine diagnostics;
	• reviewing comparative reports to identify potential system degradation;
	• confirming successful data transfer, such as the TSL;
	• confirming data transmission to and from external Interfaces;
	• correcting identified performance issues;
	• confirming primary and DR systems are synchronized;
	• monitoring backups;
	• database administration and monitoring;
	• general System health;
	• evaluating storage Requirements and

	• reviewing error logs and Alerts.
245	The Contractor shall validate that all BOS components obtain virus protection and security updates as soon as they are available.
246	The Contractor shall provide advance Notice and obtain Approval when purging jobs that permanently delete data from the system are to be executed, including but not limited to: data elements impacted, date range applied and data size impact.
247	The Contractor shall re-establish or re-install system files, programs and parameters, as required, following a failure or damage to the system and return the BOS to a fully-operational condition.
248	The Contractor shall maintain and test up-to-date Software backups (all system Software and data) in accordance with the Maintenance Plan that is secure and protects the integrity of the data.
249	The Contractor shall provide backups performed on physically separate Hardware and Software from the data being backed up.
250	The Contractor shall maintain accurate Equipment inventory status and update status.

1.2.1. BOS Hardware Maintenance

251	During the Operations and Maintenance Phase, the Contractor shall plan to regularly Upgrade all BOS environments to maintain a high-level of performance, reliability and provide for the implementation of the manufacturer's current system and security firmware/Software. These Upgrades shall be accounted for in the Contractor's Price Proposal and will not be separately paid for by the Authority over the Term of the Agreement.
252	During the Operations and Maintenance Phase, the Contractor shall Upgrade the Desktop Environments and office Equipment no less than every three (3) years to maintain a high-level of performance and reliability. These Upgrades shall be accounted for in the Contractor's Price Proposal and will not be separately paid for by the Authority over the Term of the Agreement.
253	BOS Hardware Maintenance shall include but are not limited to:
	• BOS servers, storage devices, backup devices and network Equipment at the primary BOS site, including all production and non-production BOS environments as required;
	• BOS servers, storage devices, backup devices and network Equipment at the BOS DR site;
	• all Contractor-provided desktop Hardware and peripherals;
	• all Hardware and peripherals that interact with the BOS to the extent that the Contractor-installed Software or applications are negatively affecting the operation of the peripheral;

	• all CSC office Equipment. For example, copiers and printers and
	• IVR, ACD and telephony systems.

1.2.2. BOS Network System Maintenance

254	Any Maintenance and/or replacement costs shall be included in the Contractor's Price Proposal and will not be separately paid for by the Authority over the Term of the Agreement unless explicitly noted.
255	During the Operations and Maintenance Phase, the Contractor shall plan to regularly Upgrade the network Hardware to maintain a high-level of BOS reliability and provide for the implementation of the manufacturer's current system and security firmware/Software. These Upgrades shall be included in the Contractor's Price Proposal and will not be separately paid for by the Authority over the Term of the Agreement.
256	The Contractor shall maintain and monitor the BOS network, including connection of the primary and DR BOS locations.
257	The Contractor shall proactively monitor the WAN network, its connections and its components to respond to any fault or problem.
258	The Contractor shall monitor all communications with interfacing systems and Third-Party Service Providers.
259	The Contractor shall monitor all network Alerts and alarms, as well as detect intrusion attempts and prevent intrusions.
260	The Contractor shall perform the necessary support services required of the Interoperable Agencies in order to keep day to day operations and transfers current, such as operating system Upgrades.
261	The Contractor shall Upgrade and Update the network security and provide the required Software and monitoring tools to ensure the BOS is always in compliance with the Security Standards.

1.2.3. BOS Administration and Software Support Services

262	The Contractor shall include in their Price Proposal all administration, system Maintenance and Software Maintenance costs. The Authority shall only pay for items that are explicitly identified as being paid for by the Authority. Software modifications required to maintain and support the BOS as a part of the normal course of business shall not be considered Upgrades or Enhancements paid for by the Authority. These modifications include but are not limited to:
	• Updates the System to keep up with and support new mobile devices, mobile browsers, desktop browsers and operating systems, mobile and desktop customer experience trends, mobile payments, trends in mobile device and desktop navigation techniques, as well as updated look and feel for the Self-Service Website and Self-Service Mobile Application (Phase II and optional);

	• version changes;
	• configuration or parameter changes;
	• all changes to Interoperable or CTOC ICDs and related reports;
	• all changes to ICDs and Interfaces to Contractor-selected Third-Party Service Providers;
	• minor changes to reports, Software or code;
	• Software modifications required to ensure BOS is compliant to existing Security Standards and
	• changes for the Contractor's benefit that improve the Contractor's ability to maintain and support the BOS and to meet the Performance Measures.
263	The Contractor shall provide Maintenance and Software Support Services for all elements of the BOS, including but not limited to:
	• operating systems;
	• databases;
	• BOS application Software;
	• third-party Software;
	• Software change management;
	• Software configuration management and
	• Software version control.
264	The Contractor shall maintain all secure website certificates for all websites, including the website serving the Authority managed content, if required.
265	The Contractor shall provide Maintenance and Software Support Services that include monitoring, preventive, predictive and corrective action to ensure BOS performance is in accordance with Requirements. This shall include but is not limited to:
	• any daily, weekly or periodic Maintenance required to maintain the BOS at required performance levels (such as, indexing and tuning databases and archiving and purging);
	• third-party Software or firmware patches, updates and Upgrades, as required and to be compliant with Security Standards, including but not limited to: performing security Software Upgrades, database Upgrades and operating system Upgrades;
	• Approved adjustments and updates to the BOS data based on a criteria and conditions Approved by the Authority to correct failures and issues;
	• monitoring of error logs and system logs;

	• Maintenance of back-ups and backup Software;
	• Maintenance of all BOS environments;
	• installation of new Software and confirmation of successful installation;
	• verify data replication to DR site is occurring as configured and replication is not drifting beyond an acceptable threshold;
	• verify time synchronization is occurring as configured, and system clocks are not drifting or otherwise incorrect;
	• modifications to IVR call flow needed to correct routing and call flow problems identified during normal operations;
	• creation of ad-hoc reports requested by the Authority;
	• generation of queries as requested by the Authority;
	• analysis of data as requested by the Authority and
	• modifications to the Self-Service Website and Self-Service Mobile Application (Phase II and optional) to keep up-to-date with the Authority's policies and general information.
266	Software support services shall include monitoring and corrective action to ensure BOS performance is in accordance with Requirements, to include database management and operation. This shall include but is not limited to:
	• investigation and analysis of errors and exceptions and taking corrective action, including correcting the problem and reprocessing the data;
	• monitoring notifications and initiating corrective actions on application programs to meet Requirements;
	• updates to the BOS to support Upgrades to Hardware or third-party Software and
	• updates to the BOS to support all changes to Business Rules and BOS Configurable parameters and deploy changes in production.
267	The Contractor shall monitor, Upgrade and Update the BOS is always in compliance with the Security Standards.
268	The Contractor shall ensure Maintenance does not conflict with or cause interruption in service or cause substandard service to the Authority or its customers.

1.2.4. Payment Card Industry (PCI) Security Standards and Compliance

The PCI Security Standards Council is responsible for the development, management, education and awareness of the PCI Security Standards, including the PCI DSS, Payment Application Data Security Standard (PA-DSS). The PCI Security Standards provide guidance for merchants, vendors and security consulting companies to mitigate data breaches and prevent payment cardholder data fraud.

The Contractor is responsible for ensuring that PCI compliance is fully achieved prior to the Go-Live date. The Contractor is further required to ensure that the BOS continues to be PCI compliant as outlined in the Maintenance and Operations Phase Requirements.

269	The Contractor and the BOS shall be in compliance with the appropriate PCI DSS merchant level as defined by the PCI Security Standards Council in place at the time of BOS Go-Live.
270	The Contractor shall ensure that the BOS is in compliance with any individual additions to the PCI Security Standards since the last major version or the current version published by the PCI Security Standards Council and all future versions.
271	The Contractor shall utilize the PCI Security Standards Council's Prioritized Approach method to indicate how each PCI Requirement is being addressed prior to Go-Live. The Prioritized Approach shall be submitted to the Authority along with substantiating evidence for review and Approval.
272	The Contractor shall ensure the BOS is in compliance with PCI-DSS for any Commercial Off-the-Shelf (COTS) Software that will be used in payment applications.
273	The Contractor shall provide, prior to the BOS Go-Live:
	• PCI Attestation of compliance by either a qualified ISA or an independent QSA, or as required by PCI DSS;
	• vulnerability scan by an Approved scanning vendor and
	• internal and external penetration testing results.
274	No more than three (3) months after Go-Live the Contractor shall provide a complete Report of Compliance (ROC), including details about the BOS environment and the assessment methodology, as well as documentation regarding the BOS's compliance status for each PCI DSS Requirement. The ROC shall be provided which outlines a clear plan and schedule (in writing) to achieve full PCI compliance no more than six (6) months after Go-Live.
275	The Contractor shall be responsible for providing a ROC prior to BOS Acceptance.

1.2.5. Interoperability Requirements

The Authority currently has Interoperability agreements with CTOC Agencies and, in the future, it is anticipated that regional and national Interoperable agreements will be established. These Requirements apply to all existing and future Interoperability.

Interoperability includes exchanging and processing transactions/trips, customer, transponder, payment, corrections, vehicle data, invoices and reconciliations between the BOS and the Interoperable Agencies. The BOS shall process transactions/trips from Interoperable Agencies for the Authority's customers who have used Interoperable Agency roads, as well as transactions/trips for Interoperable Agencies' customers on the Authority's facility. The Interface supports the transmission and receipt of all files identified in the respective ICDs.

At the Authority's direction, the Contractor shall support direct connection and/or connection through a CTOC Agency intermediary to nationally (non-CTOC) Interoperable Agencies.