OKLAHOMA
Office of Management
& Enterprise Services

State of Oklahoma

Office of Management and Enterprise Services

STATE OF OKLAHOMA CONTRACT WITH EXPLORE INFORMATION SERVICES, LLC

This State of Oklahoma Contract is entered into between the State of Oklahoma by and through the Office of Management and Enterprise Services ("State") for the benefit of the Oklahoma Corporation Commission ("Customer" or "OCC") and Explore Information Services, LLC ("Supplier") and is effective as of the effective date set forth on a properly issued purchase order or, if no effective date is listed, the date of last signature to this Contract ("Effective Date"). The initial term of the Contract shall be for one (1) year with nine (9) one-year options to renew.

Purpose

The State is awarding this Contract to Supplier for the provision of an International Fuel Tax Agreement, International Registration Plan, ("IFTA/IRP") System as more particularly described in certain Contract Documents. Supplier requested confidential matters to be considered. This Contract memorializes the agreement of the parties with respect to negotiated terms of the Contract that is being awarded to Supplier.

Now, therefore, in consideration of the foregoing and the mutual promises set forth herein, the receipt and sufficiency of which are hereby acknowledged the parties agree as follows:

1. The parties agree that Supplier has not yet begun performance of work under this Contract. Issuance of a purchase order is required prior to payment to a Supplier.
2. The following Contract Documents are attached hereto and incorporated herein:

   2.1. Solicitation #EV00000780, Attachment A;
   2.2. State of Oklahoma General Terms, Attachment B;
   2.3. Agency Terms, Attachment C;
   2.4. Information Technology Terms, Attachment D;
   2.5. Response to Specifications and Requirements, Attachment E;
   2.6. Pricing, Attachment E-1;
   2.7. Intentionally Omitted, Attachment E-2, and
   2.8. Value Add, Attachment E-3

3. The parties additionally agree:

   3.2. Except for the IT Security Certification and information deemed confidential by the State pursuant to applicable law, rule, regulation or policy, the parties agree Contract terms and information are not confidential and are disclosable without further approval of or notice to Supplier.

   3.3. To the extent any term or condition in any Contract Document, including via a hyperlink or uniform resource locator, conflicts with an applicable Oklahoma and/or United States law or regulation, such term or condition is void and unenforceable. By executing any

Contract Document which contains a conflicting term or condition, the State or Customer makes no representation or warranty regarding the enforceability of such term or condition and the State or Customer does not waive the applicable Oklahoma and/or United States law or regulation which conflicts with the term or condition.

4. Payment obligations rest solely with the OCC. Please send invoices and billing inquiries to:

Oklahoma Corporation Commission
2401 North Lincoln Boulevard,
Oklahoma City, Oklahoma 73105
Email: occaccountspayable@occ.ok.gov

5. Attachments referenced in this section are attached hereto and incorporated herein.

6. Any reference to a Contract Document refers to such Contract Document as it may have been amended. If and to the extent any provision is in multiple documents and addresses the same or substantially the same subject matter but does not create an actual conflict, the more recent provision is deemed to supersede earlier versions.

7. The undersigned Agency hereby attests that any required terms and conditions based on a Federal Award applicable to this Contract are included herein.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

SIGNATURES

The undersigned represent and warrant that they are authorized, as representatives of the party on whose behalf they are signing, to sign this Contract and to bind their respective party thereto.

STATE OF OKLAHOMA
by and through the CORPORATION COMMISSION:

By: Jim Marshall
Jim Marshall (May 5, 2026 12:08:18 CDT)

Name: Jim Marshall

Title: Oklahoma Corporation Commission Appointing Authority

Date: May 5, 2026

EXPLORE INFORMATION SERVICES, LLC:

By: Tom Eggenberger
Tom Eggenberger (Apr 10, 2026 13:46:36 CDT)

Name: Tom Eggenberger

Title: Government Solutions Product Owner

Date: Apr 10, 2026

Agency Counsel

By: Pat Franz
Pat Franz (May 5, 2026 10:05:39 CDT)

Name: Pat Franz

Title: General Counsel III

Date: May 5, 2026

The Chief Information Officer is signing solely to approve the Contract pursuant to 62 O.S., § 34.11.1 concerning procurement of Information Technology and/or Telecommunications.

By:
Dan Cronin (May 5, 2026 12:31:24 CDT)

Name: Dan Cronin

Title: Chief Information Officer/Chief Transformation Officer

Date: May 5, 2026

Attachment A
Agency Solicitations
Solicitation No. EV00000780

This Solicitation is a Contract Document and is a request for proposal in connection with the Contract awarded on behalf of Oklahoma Corporation Commission by and through the Office of Management and Enterprise Services as more particularly described below. Any defined term used herein but not defined herein shall have the meaning ascribed in the General Terms or other Contract document.

I. PURPOSE

The Office of Management and Enterprise Services (OMES), Central Purchasing Division, is seeking responses on behalf of Oklahoma Corporation Commission (OCC) from potential Suppliers to provide a contract for the purchase of a new International Fuel Tax Agreement (IFTA)/International Registration Plan (IRP) System. A Contract resulting from this Solicitation may be designated for use as a Statewide Contract.[1]

The Contract is awarded on behalf of Oklahoma Corporation Commission for a New IFTA/IRP System.

1. Contract Term and Renewal Options:

1.1. The initial Contract term, which begins on the effective date of the Contract, is one year and there are nine (9) one-year options to renew the Contract.

2. Solicitation Criterion:

2.1. The Bid will be evaluated using Best Value Criterion, based on the following:

2.1.1. Price
2.1.2. Past performance
2.1.3. Ability to supply products
2.1.4. Mandatory Specifications

3. Scope and Description:

3.1. The Bid Response must reflect for each requirement on Exhibit-04: Mandatory Specifications whether the requirement is met by an out-of-the-box solution or whether the requirement necessitates customization to the Bidder's proposed solution.

[1] 74 O.S. 85.5(G)(3)

3.2. The Bid Response shall show the ability of the Bidder to meet or exceed the following mandatory specifications: Exhibit-04: Mandatory Specifications Technical Response Worksheet

3.3. OCC would like a demonstration of the potential IFTA/IRP system that the bidder has built in the past for other state entities or agencies.

4. **Pricing**

4.1. Pricing shall be proposed utilizing deliverable-based pricing with proposed milestones and associated payments. Ongoing subscription costs are provided as part of the TCO sheet for scoring.

4.2. Value-added products and/or services within scope of the Acquisition may be included in the Bid.

5. **Executive Summary and Company Information are on Exhibit-01: Executive Summary and Company Information.**

6. **All Technical responses are on Exhibit-04: Mandatory Specifications Technical Response Worksheet**

7. **The response to pricing shall be proposed using Exhibit-02: Price Template.**

8. **Value-added products and/or services within scope of the Acquisition are to be included in Exhibit-04: Mandatory Specifications Technical Response Worksheet.**

9. **Business References are to be on Exhibit-03: Bidder Reference Worksheet.**

10. **Mandatory Specifications are to be on Exhibit-04: Mandatory Specifications Technical Response Worksheet**

ATTACHMENT B

STATE OF OKLAHOMA GENERAL TERMS

This State of Oklahoma General Terms ("General Terms") is a Contract document in connection with the Contract awarded by the State of Oklahoma by and through the Office of Management and Enterprise Services.

In addition to other terms contained in an applicable Contract document, Supplier and State agree to the following General Terms:

1 Scope and Contract Renewal

1.1 Supplier may not add products or services to its offerings under the Contract without the State's prior written approval. Such request may require a competitive bid of the additional products or services. If the need arises for goods or services outside the scope of the Contract, Supplier shall contact the State.

1.2 At no time during the performance of the Contract shall the Supplier have the authority to obligate any Customer for payment for any products or services (a) when a corresponding encumbering document is not signed or (b) over and above an awarded Contract amount. Likewise, Supplier is not entitled to compensation for a product or service provided by or on behalf of Supplier that is neither requested nor accepted as satisfactory.

1.3 If applicable, prior to any Contract renewal, the State shall subjectively consider the value of the Contract to the State, the Supplier's performance under the Contract, and shall review certain other factors, including but not limited to the: a) terms and conditions of Contract documents to determine validity with current State and other applicable statutes and rules; b) current pricing and discounts offered by Supplier; and c) current products, services and support offered by Supplier. If the State determines changes to the Contract are required as a condition precedent to renewal, the State and Supplier will cooperate in good faith to evidence such required changes in an Amendment. Further, any request for a price increase in connection with a renewal or otherwise will be conditioned on the Supplier providing appropriate documentation supporting the request.

1.4 The State may extend the Contract for ninety (90) days beyond a final renewal term at the Contract compensation rate for the extended period. If the State exercises such option to extend ninety (90) days, the State shall notify the Supplier in writing prior to Contract end date. The State, at its sole option and to the extent allowable by law, may choose to exercise subsequent ninety (90) day extensions at the Contract pricing rate, to facilitate the finalization of related terms and conditions of a new award or as needed for transition to a new Supplier.

1.5 Supplier understands that supplier registration expires annually and, pursuant to OAC 260:115-3-3, Supplier shall maintain its supplier registration with the State as a precondition to a renewal of the Contract.

2 Contract Effectiveness and Order of Priority

2.1 Unless specifically agreed in writing otherwise, the Contract is effective upon the date last signed by the parties. Supplier shall not commence work, commit funds, incur costs, or in any way act to obligate the State until the Contract is effective.

2.2 Contract documents shall be read to be consistent and complementary. Any conflict among the Contract documents shall be resolved by giving priority to Contract documents in the following order of precedence:

A. any Amendment;

B. terms contained in this Contract document

C. any Contract-specific State terms including, without limitation, information technology terms and terms specific to a statewide Contract or a State agency Contract;

D. any applicable Solicitation;

E. any successful Bid as may be amended through negotiation and to the extent the Bid does not otherwise conflict with the Solicitation or applicable law;

F. any statement of work, work order, or other mutually agreed Contract documents.

2.3 If there is a conflict between the terms contained in this Contract document or in Contract-specific terms and an agreement provided by or on behalf of Supplier including but not limited to linked or supplemental documents which alter or diminish the rights of Customer or the State, the conflicting terms provided by Supplier shall not take priority over this Contract document or Acquisition-specific terms. In no event will any linked document alter or override such referenced terms except as specifically agreed in an Amendment.

2.4 Any Contract document shall be legibly written in ink or typed. All Contract transactions, and any Contract document related thereto, may be conducted by electronic means pursuant to the Oklahoma Uniform Electronic Transactions Act.

3 Modification of Contract Terms and Contract documents

3.1 The Contract may only be modified, amended, or expanded by an Amendment. Any change to the Contract, including the addition of work or materials, the revision of payment terms, or the substitution of work or materials made unilaterally by the Supplier, is a material breach of the Contract. Unless otherwise specified by applicable law or rules, such changes, including without limitation, any unauthorized written Contract modification, shall be void and without effect and the Supplier shall not be entitled to any claim under the Contract based on those changes. No oral statement of any person shall modify or otherwise affect the terms, conditions, or specifications stated in the Contract.

3.2 Any additional terms on an ordering document provided by Supplier are of no effect and are void unless mutually executed. OMES bears no liability for performance, payment or failure thereof by the Supplier or by a Customer other than OMES in connection with an Acquisition.

3.3 Except for information deemed confidential by the State pursuant to applicable law, rule, regulation, or policy, the parties agree Contract terms and information are not confidential and are disclosable without further approval of or notice to Supplier.

3.4 Unless mutually agreed to in writing by the State of Oklahoma by and through the Office of Management and Enterprise Services, no Contract document or other terms and conditions or clauses, including via a hyperlink or uniform resource locator, shall supersede or conflict with the terms of this Contract or expand the State's or Customer's liability or reduce the rights of Customer or the State. If Supplier is acting as a reseller, any third-party terms provided are also subject to the foregoing.

3.5 To the extent any term or condition in any Contract document, including via a hyperlink or uniform resource locator, conflicts with an applicable Oklahoma and/or United States law or regulation, such term or condition is void and unenforceable. By executing any Contract document which contains a conflicting term or condition, the State or Customer makes no representation or warranty regarding the enforceability of such term or condition and the State or Customer does not waive the applicable Oklahoma and/or United States law or regulation which conflicts with the term or condition.

4 Definitions

In addition to any defined terms set forth elsewhere in the Contract, the Oklahoma Central Purchasing Act and the Oklahoma Administrative Code, Title 260, the parties agree that, when used in the Contract, the following terms are defined as set forth below and may be used in the singular or plural form:

4.1 **Acquisition** means items, products, materials, supplies, services and equipment acquired by purchase, lease purchase, lease with option to purchase, value provided or rental under the Contract.

4.2 **Amendment** means a mutually executed, written modification to a Contract document.

4.3 **Bid** means an offer a Bidder submits in response to the Solicitation.

4.4 **Bidder** means an individual or business entity that submits a Bid in response to the Solicitation.

4.5 **Contract** means the written, mutually agreed and binding legal relationship resulting from the Contract documents and an appropriate encumbering document as may be amended from time to time, which evidences the final agreement between the parties with respect to the subject matter of the Contract.

4.6 **Customer** means the governmental entity receiving goods or services contemplated by the Contract.

4.7 **Debarment** means action taken by a debarring official under federal or state law or regulations to exclude any business entity from inclusion on the Supplier list; bidding; offering to bid; providing a quote; receiving an award of contract with the State and may also result in cancellation of existing contracts with the State.

4.8 **Destination** means delivered to the receiving dock or other point specified in the applicable Contract document.

4.9 **Governmental Entity** means any governmental entity specified as a political subdivision of the State pursuant to the Governmental Tort Claim Act including any associated institution, instrumentality, board, commission, committee, department, or other entity designated to act on behalf of the state.

4.10 **Indemnified Parties** means the State and Customer and/or its officers, directors, agents, employees, representatives, contractors, assignees, and designees thereof.

4.11 **Inspection** means examining and testing an Acquisition (including, when appropriate, raw materials, components, and intermediate assemblies) to determine whether the Acquisition meets Contract requirements.

4.12 **Moral Rights** means any and all rights of paternity or integrity of the Work Product and the right to object to any modification, translation or use of the Work Product and any similar rights existing under the judicial or statutory law of any country in the world or under any treaty, regardless of whether or not such right is denominated or referred to as a moral right.

4.13 **OAC** means the Oklahoma Administrative Code.

4.14 **OMES** means the Office of Management and Enterprise Services.

4.15 **Solicitation** means the document inviting Bids for the Acquisition referenced in the Contract and any amendments thereto.

4.16 **State** means the government of the state of Oklahoma, its employees and authorized representatives, including without limitation any department, agency, or other unit of the government of the state of Oklahoma.

4.17 **Supplier** means the Bidder with whom the State enters into the Contract awarded pursuant to the Solicitation or the business entity or individual that is a party to the Contract with the State.

4.18 **Suspension** means action taken by a suspending official under federal or state law or regulations to suspend a Supplier from inclusion on the Supplier list; be eligible to submit Bids to State agencies and be awarded a contract by a State agency subject to the Central Purchasing Act.

4.19 **Supplier Confidential Information** means certain confidential and proprietary information of Supplier that is clearly marked as confidential and agreed by the State Purchasing Director or Customer, as applicable, but does not include information excluded from confidentiality in provisions of the Contract or the Oklahoma Open Records Act.

4.20 **Work Product** means any and all deliverables produced by Supplier under a statement of work or similar Contract document issued pursuant to this Contract, including any and all tangible or intangible items or things that have been or will be prepared, created, developed, invented or conceived at any time following the Contract effective date including but not limited to any (i) works of authorship (such as manuals, instructions, printed material, graphics, artwork, images, illustrations, photographs, computer programs, computer software, scripts, object code, source code or other programming code, HTML code, flow charts, notes, outlines, lists, compilations, manuscripts, writings, pictorial materials, schematics, formulae, processes, algorithms, data, information, multimedia files, text web pages or web sites, other written or machine readable expression of such works fixed in any tangible media, and all other copyrightable works), (ii) trademarks, service marks, trade dress, trade names, logos, or other indicia of source or origin, (iii) ideas, designs, concepts, personality rights, methods, processes, techniques, apparatuses, inventions, formulas, discoveries, or improvements, including any patents, trade secrets and know-how, (iv) domain names, (v) any copies, and similar or derivative works to any of the foregoing, (vi) all documentation and materials related to any of the foregoing, (vii) all other goods, services or deliverables to be provided by or on behalf of Supplier under the Contract and (vii) all Intellectual Property Rights in any of the foregoing, and which are or were created, prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or with funds appropriated by or for Customer or Customer's benefit (a) by any Supplier personnel or Customer personnel or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

5 Pricing

5.1 Pursuant to 68 O.S. §§ 1352, 1356, and 1404, State agencies are exempt from the assessment of State sales, use, and excise taxes. Further, State agencies and political subdivisions of the State are exempt from Federal Excise Taxes pursuant to Title 26 of the United States Code. Any taxes of any nature whatsoever payable by the Supplier shall not be reimbursed.

5.2 Pursuant to 74 0. S. § 85.40, all travel expenses of Supplier must be included in the total Acquisition price.

5.3 The price of a product offered under the Contract shall include and Supplier shall prepay all shipping, packaging, delivery and handling fees. All product deliveries will be free on-board Customer's Destination. No additional fees shall be charged by Supplier for standard shipping and handling. If Customer requests expedited or special delivery, Customer may be responsible for any charges for expedited or special delivery.

6 Ordering, Inspection, and Acceptance

6.1 Any product or service furnished under the Contract shall be ordered by issuance of a valid purchase order or other appropriate payment mechanism, including a pre-encumbrance, or by use of a valid Purchase Card. All orders and transactions are governed by the terms and conditions of the Contract. Any purchase order or other applicable payment mechanism dated prior to termination or expiration of the Contract shall be performed unless mutually agreed in writing otherwise.

6.2 Services will be performed in accordance with industry best practices and are subject to acceptance by the Customer. Notwithstanding any other provision in the Contract, deemed acceptance of a service or associated deliverable shall not apply automatically upon receipt of a deliverable or upon provision of a service. Supplier warrants and represents that a product or deliverable furnished by or through the Supplier shall individually, and where specified by Supplier to perform as a system, be substantially uninterrupted and error-free in operation and guaranteed against faulty material and workmanship for a warranty period of the greater of ninety (90) days from the date of acceptance or the maximum allowed by the manufacturer. A defect in a product or deliverable furnished by or through the Supplier shall be repaired or replaced by Supplier at no additional cost or expense to the Customer if such defect occurs during the warranty period.

Any product to be delivered pursuant to the Contract shall be subject to final inspection and acceptance by the Customer at Destination. The Customer assumes no responsibility for a product until accepted by the Customer. Title and risk of loss or damage to a product shall be the responsibility of the Supplier until accepted. The Supplier shall be responsible for filing, processing, and collecting any and all damage claims accruing prior to acceptance.

Pursuant to OAC 260:115-9-1, payment for an Acquisition does not constitute final acceptance of the Acquisition. If subsequent inspection affirms that the Acquisition does not meet or exceed the specifications of the order or that the Acquisition has a latent defect, the Supplier shall be notified as soon as is reasonably practicable. The Supplier shall retrieve and replace the Acquisition at Supplier's expense or, if unable to replace, shall issue a refund to Customer. Refund under this section shall not be an exclusive remedy.

6.3 Supplier shall deliver products and services on or before the required date specified in a Contract document. Failure to deliver timely may result in liquidated damages as set forth in the applicable Contract document. Deviations, substitutions, or changes in a product or service, including changes of personnel directly providing services, shall not be made unless expressly authorized in writing by the Customer. Any substitution of personnel directly providing services shall be a person of comparable or greater skills, education and experience for performing the services as the person being replaced. Additionally, Supplier shall provide staff sufficiently experienced and able to perform with respect to any transitional services provided by Supplier in connection with termination or expiration of the Contract.

6.4 Product warranty and return policies and terms provided under any Contract document will not be more restrictive or more costly than warranty and return policies and terms for other similarly situated customers for a like product.

7 Invoices and Payment

7.1 Supplier shall be paid upon submission of a proper invoice(s) at the prices stipulated in the Contract in accordance with 74 O.S. §85.44B which requires that payment be made only after products have been provided and accepted or services rendered and accepted.

The following terms additionally apply:

A. An invoice shall contain the purchase order number, description of products or services provided and the dates of such provision.

B. Failure to provide a timely and proper invoice may result in delay of processing the invoice for payment. Proper invoice is defined at OAC 260:10-1-2.

C. Payment of all fees under the Contract shall be due NET 45 days. Payment and interest on late payments are governed by 62 O.S. §34.72. Such interest is the sole and exclusive remedy for late payments by a State agency and no other late fees are authorized to be assessed pursuant to Oklahoma law.

D. The date from which an applicable early payment discount time is calculated shall be from the receipt date of a proper invoice. There is no obligation, however, to utilize an early payment discount.

E. If an overpayment or underpayment has been made to Supplier any subsequent payments to Supplier under the Contract may be adjusted to correct the account. A written explanation of the adjustment will be issued to Supplier.

F. Supplier shall have no right of setoff.

G. Because funds are typically dedicated to a particular fiscal year, an invoice will be paid only when timely submitted, which shall in no instance be later than six (6) months after the end of the fiscal year in which the goods are provided or services performed.

H. The Supplier shall accept payment by Purchase Card as allowed by Oklahoma law.

8 Maintenance of lnsurance, Payment of Taxes, and Workers' Compensation

8.1 As a condition of this Contract, Supplier shall procure at its own expense, and provide proof of, insurance coverage with the applicable liability limits set forth below and any approved subcontractor of Supplier shall procure and provide proof of the same coverage. The required insurance shall be underwritten by an insurance carrier with an A.M. Best rating of A- or better. Such proof of coverage shall additionally be provided to the Customer if services will be provided by any of Supplier's employees, agents or subcontractors at any Customer premises and/or employer vehicles will be used in connection with performance of Supplier's obligations under the Contract. Supplier may not commence performance hereunder until such proof has been provided. Additionally, Supplier shall ensure each insurance policy includes a notice of cancellation and includes the State and its agencies as certificate holder and shall promptly provide proof to the State of any renewals, additions, or changes to such insurance coverage. Supplier's obligation to maintain insurance coverage under the Contract is a continuing obligation until Supplier has no further obligation under the Contract. Any combination of primary and excess or umbrella insurance may be used to satisfy the limits of coverage for Commercial General Liability, Auto Liability and Employers' Liability. Unless agreed between the parties and approved by the State Purchasing Director, the minimum acceptable insurance limits of liability are as follows:

A. Workers' Compensation and Employer's Liability Insurance in accordance with and to the extent required by applicable law;

B. Commercial General Liability Insurance covering the risks of personal injury, bodily injury (including death) and property damage, including coverage for contractual liability, with a limit of liability of not less than 2,000,000 per occurrence;

C. Automobile Liability Insurance with limits of liability of not less than $2,000,000 combined single limit each accident;

D. If the Supplier will access, process, or store state data, then Security and Privacy Liability insurance, including coverage for failure to protect confidential information and failure of the security of Supplier's computer systems that results in unauthorized access to Customer data with a limit of not less than $5,000,000 per occurrence; and

E. Additional coverage required in writing in connection with a particular Acquisition.

8.2 Supplier shall be entirely responsible during the existence of the Contract for the liability and payment of taxes payable by or assessed to Supplier or Supplier's employees, agents and subcontractors of whatever kind, in connection with the Contract. Supplier further agrees to comply with all state and federal laws applicable to any such persons, including laws regarding wages, taxes, insurance, and Workers' Compensation. Neither Customer nor the State shall be liable to the Supplier, Supplier's employees, agents, or others for the payment of taxes or the provision of unemployment insurance and/or Workers' Compensation or any benefit available to a State or Customer employee.

8.3 Supplier agrees to indemnify Customer, the State, and its employees, agents, representatives, contractors, and assignees for any and all liability, actions, claims, demands, or suits, and all related costs and expenses (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) relating to tax liability, unemployment insurance and/or Workers' Compensation in connection with its performance under the Contract.

9 Compliance With Applicable Laws

9.1 As long as Supplier has an obligation under the terms of the Contract and in connection with performance of its obligations, the Supplier represents its present compliance, and shall have an ongoing obligation to comply, with all applicable federal, State, and local laws, rules, regulations, ordinances, and orders, as amended, including but not limited to the following:

A. Drug-Free Workplace Act of 1988 set forth at 41 U.S.C. §81.

B. Section 306 of the Clean Air Act, Section 508 of the Clean Water Act, Executive Order 11738, and Environmental Protection Agency Regulations which prohibit the use of facilities included on the EPA List of Violating Facilities under nonexempt federal contracts, grants or loans;

C. Prospective participant requirements set at 2 C.F.R. part 376 in connection with Debarment, Suspension and other responsibility matters;

D. 1964 Civil Rights Act, Title IX of the Education Amendment of 1972, Section 504 of the Rehabilitation Act of 1973, and Americans with Disabilities Act of 1990;

E. Anti-Lobbying Law set forth at 31 U.S.C. §1325 and as implemented at 45 C.F.R. part 93;

F. Requirements of Internal Revenue Service Publication 1075 regarding use, access and disclosure of Federal Tax Information (as defined therein);

G. Obtaining certified independent audits conducted in accordance with Government Auditing Standards and Office of Management and Budget Uniform Guidance, 2 CFR 200 Subpart F §200.500 et seq. with approval and work paper examination rights of the applicable procuring entity;

H. Requirements of the Oklahoma Taxpayer and Citizen Protection Act of 2007, 25 O.S. § 1312 and applicable federal immigration laws and regulations and be registered and participate in the Status Verification System. The Status Verification System is defined at 25 O.S. § 1312, includes but is not limited to the free Employment Verification Program (E-Verify) through the Department of Homeland Security, and is available at e-verify.gov.

I. Requirements of the Health Insurance Portability and Accountability Act of 1996; Health Information Technology for Economic and Clinical Health Act; Payment Card Industry Security Standards; Criminal Justice Information System Security Policy and Security Addendum; and Family Educational Rights and Privacy Act; and

J. Be registered as a business entity licensed to do business in the State, have obtained a sales tax permit, and be current on franchise tax payments to the State, as applicable.

9.2 The Supplier's employees, agents and subcontractors shall adhere to applicable Customer policies including, but not limited to acceptable use of Internet and electronic mail, facility and data security, press releases, and public relations. As applicable, the Supplier shall adhere to the State Information Security Policy, Procedures, Guidelines set forth at e-verify.gov. Supplier is responsible for reviewing and relaying such policies covering the above to the Supplier's employees, agents and subcontractors.

9.3 At no additional cost to Customer, the Supplier shall maintain all applicable licenses and permits required in association with its obligations under the Contract.

9.4 In addition to compliance under subsection 9.1 above, Supplier shall have a continuing obligation to comply with applicable Customer-specific mandatory contract provisions required in connection with the receipt of federal funds or other funding source.

9.5 The Supplier is responsible to review and inform its employees, agents, and subcontractors who provide a product or perform a service under the Contract of the Supplier's obligations under the Contract and Supplier certifies that its employees and each such subcontractor shall comply with minimum requirements and applicable provisions of the Contract. At the request of the State, Supplier shall promptly provide adequate evidence that such persons are its employees, agents or approved subcontractors and have been informed of their obligations under the Contract.

9.6 As applicable, Supplier agrees to comply with the Governor's Executive Orders related to the use of any tobacco product, electronic cigarette or vaping device on any and all properties owned, leased, or contracted for use by the State, including but not limited to all buildings, land and vehicles owned, leased, or contracted for use by agencies or instrumentalities of the State.

9.7 The execution, delivery and performance of the Contract and any ancillary documents by Supplier will not, to the best of Supplier's knowledge, violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third party.

9.8 Supplier represents that it has the ability to pay its debts when due and it does not anticipate the filing of a voluntary or involuntary bankruptcy petition or appointment of a receiver, liquidator or trustee.

9.9 Supplier represents that, to the best of its knowledge, any litigation or claim or any threat thereof involving Supplier has been disclosed in writing to the State and Supplier is not aware of any other litigation, claim or threat thereof.

9.10 If services provided by Supplier include delivery of an electronic communication, Supplier shall ensure such communication and any associated support documents are compliant with Section 508 of the Federal Rehabilitation Act and with State standards regarding accessibility. Should any communication or associated support documents be non-compliant, Supplier shall correct and re-deliver such communication immediately upon discovery or notice, at no additional cost to the State. Additionally, as part of compliance with accessibility requirements where documents are only provided in non- electronic format, Supplier shall promptly provide such communication and any associated support documents in an alternate format usable by individuals with disabilities upon request and at no additional cost, which may originate from an intended recipient or from the State.

10 Audits and Records Clause

10.1 As used in this clause and pursuant to 67 O.S. §203, "record" includes a document, book, paper, photograph, microfilm, computer tape, disk, record, sound recording, film recording, video record, accounting procedures and practices, and other data, regardless of type and regardless of whether such items are in written form, in the form of computer data, or in any other form. Supplier agrees any pertinent federal or State agency or governing entity of a Customer shall have the right to examine and audit, at no additional cost to a Customer, all records relevant to the execution and performance of the Contract except, unless otherwise agreed, costs of Supplier that comprise pricing under the Contract.

10.2 The Supplier is required to retain records relative to the Contract for the duration of the Contract and for a period of seven (7) years following completion or termination of an Acquisition unless otherwise indicated in the Contract terms. If a claim, audit, litigation or other action involving such records is started before the end of the seven-year period, the records are required to be maintained for two (2) years from the date that all issues arising out of the action are resolved, or until the end of the seven (7) year retention period, whichever is later.

10.3 Pursuant to 74 O.S. § 85.41, if professional services are provided hereunder, all items of the Supplier that relate to the professional services are subject to examination by the State agency, State Auditor and Inspector and the State Purchasing Director.

11 Confidentiality

11.1 The Supplier shall maintain strict security of all State and citizen data and records entrusted to it or to which the Supplier gains access, in accordance with and subject to applicable federal and State laws, rules, regulations, and policies and shall use any such data and records only as necessary for Supplier to perform its obligations under the Contract. The Supplier further agrees to evidence such confidentiality obligation in a separate writing if required under such applicable federal or State laws, rules and regulations. The Supplier warrants and represents that such information shall not be sold, assigned, conveyed, provided, released, disseminated or otherwise disclosed by Supplier, its employees, officers, directors, subsidiaries, affiliates, agents, representatives, assigns, subcontractors, independent contractors, successor or any other persons or entities without Customer's prior express written permission. Supplier shall instruct all such persons and entities that the confidential information shall not be disclosed or used without the Customer's prior express written approval except as necessary for Supplier to render services under the Contract. The Supplier further warrants that it has a tested and proven system in effect designed to protect all confidential information.

11.2 Supplier shall establish, maintain and enforce agreements with all such persons and entities that have access to State and citizen data and records to fulfill Supplier's duties and obligations under the Contract and to specifically prohibit any sale, assignment, conveyance, provision, release, dissemination or other disclosure of any State or citizen data or records except as required by law or allowed by written prior approval of the Customer.

11.3 Supplier shall immediately report to the Customer any and all unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State or citizen data or records of which it or its parent company, subsidiaries, affiliates, employees, officers, directors, assignees, agents, representatives, independent contractors, and subcontractors is aware or have knowledge or reasonably should have knowledge. The Supplier shall also promptly furnish to Customer full details of the unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination, or attempt thereof, and use its best efforts to assist the Customer in investigating or preventing the reoccurrence of such event in the future. The Supplier shall cooperate with the Customer in connection with any litigation and investigation deemed necessary by the Customer to protect any State or citizen data and records and shall bear all costs associated with the investigation, response and recovery in connection with any breach of State or citizen data or records including but not limited to credit monitoring services with a term of at least three (3) years, all notice-related costs and toll free telephone call center services.

11.4 Supplier further agrees to promptly prevent a reoccurrence of any unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of State or citizen data and records.

11.5 Supplier acknowledges that any improper use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State data or records to others may cause immediate and irreparable harm to the Customer and certain beneficiaries and may violate state or federal laws and regulations. If the Supplier or its affiliates, parent company, subsidiaries, employees, officers, directors, assignees, agents, representatives, independent contractors, and subcontractors improperly use, appropriate, sell, assign, convey, provide, release, access, acquire, disclose or otherwise disseminate such confidential information to any person or entity in violation of the Contract, the Customer will immediately be entitled to injunctive relief and/or any other rights or remedies available under this Contract, at equity or pursuant to applicable statutory, regulatory, and common law without a cure period.

11.6 The Supplier shall immediately forward to the State Purchasing Director, and any other applicable person listed in the Notices section(s) of the Contract, any request by a third party for data or records in the possession of the Supplier or any subcontractor or to which the Supplier or subcontractor has access and Supplier shall fully cooperate with all efforts to protect the security and confidentiality of such data or records in response to a third party request.

11.7 Customer may be provided access to Supplier's Confidential Information. State agencies are subject to the Oklahoma Open Records Act and Supplier acknowledges information marked confidential information will be disclosed to the extent permitted under the Open Records Act and in accordance with this Contract.

11.8 Except for information deemed confidential by the State pursuant to applicable law, rule, regulation, or policy, the parties agree Contract terms and information are not confidential and are disclosable without further approval of or notice to the Supplier.

12 Conflict of Interest

In addition to any requirement of law or of a professional code of ethics or conduct, the Supplier, its employees, agents and subcontractors are required to disclose any outside activity or interest that conflicts or may conflict with the best interest of the State. Prompt disclosure is required under this section if the activity or interest is related, directly or indirectly, to any person or entity currently under contract with or seeking to do business with the State, its employees or any other third-party individual or entity awarded a contract with the State. Further, as long as the Supplier has an obligation under the Contract, any plan, preparation or engagement in any such activity or interest shall not occur without prior written approval of the State. Any conflict of interest shall, at the sole discretion of the State, be grounds for partial or whole termination of the Contract.

13 Assignment and Permitted Subcontractors

13.1 Supplier's obligations under the Contract may not be assigned or transferred to any other person or entity without the prior written consent of the State which may be withheld at the State's sole discretion. Should Supplier assign its rights to payment, in whole or in part, under the Contract, Supplier shall provide the State and all affected Customers with written notice of the assignment. Such written notice shall be delivered timely and contain details sufficient for affected Customers to perform payment obligations without any delay caused by the assignment.

13.2 Notwithstanding the foregoing, the Contract may be assigned by Supplier to any corporation or other entity in connection with a merger, consolidation, sale of all equity interests of the Supplier, or a sale of all or substantially all of the assets of the Supplier to which the Contract relates. In any such case, said corporation or other entity shall by operation of law or expressly in writing assume all obligations of the Supplier as fully as if it had been originally made a party to the Contract. Supplier shall give the State and all affected Customers prior written notice of said assignment. Any assignment or delegation in violation of this subsection shall be void.

13.3 If the Supplier is permitted to utilize subcontractors in support of the Contract, the Supplier shall remain solely responsible for its obligations under the terms of the Contract, for its actions and omissions and those of its agents, employees and subcontractors and for payments to such persons or entities. Prior to a subcontractor being utilized by the Supplier, the Supplier shall obtain written approval of the State of such subcontractor and each employee, as applicable to a particular Acquisition, of such subcontractor proposed for use by the Supplier. Such approval is within the sole discretion of the State. Any proposed subcontractor shall be identified by entity name, and by employee name, if required by the particular Acquisition, in the applicable proposal and shall include the nature of the services to be performed. As part of the approval request, the Supplier shall provide a copy of a written agreement executed by the Supplier and subcontractor setting forth that such subcontractor is bound by and agrees, as applicable, to perform the same covenants and be subject to the same conditions and make identical certifications to the same facts and criteria, as the Supplier under the terms of all applicable Contract documents. Supplier agrees that maintaining such agreement with any subcontractor and obtaining prior written approval by the State of any subcontractor and associated employees shall be a continuing obligation. The State further reserves the right to revoke approval of a subcontractor or an employee thereof in instances of poor performance, misconduct or for other similar reasons.

13.4 All payments under the Contract shall be made directly to the Supplier, except as provided in 13.1 above regarding the Supplier's assignment of payment. No payment shall be made to the Supplier for performance by unapproved or disapproved employees of the Supplier or a subcontractor.

13.5 Rights and obligations of the State or a Customer under the terms of this Contract may be assigned or transferred, at no additional cost, to other Customer entities.

14 Background Checks and Criminal History Investigations

Prior to the commencement of any services, background checks and criminal history investigations of the Supplier's employees and subcontractors who will be providing services may be required and, if so, the required information shall be provided to the State in a timely manner. Supplier's access to facilities, data and information may be withheld prior to completion of background verification acceptable to the State. The costs of additional background checks beyond Supplier's normal hiring practices shall be the responsibility of the Customer unless such additional background checks are required solely because Supplier will not provide results of its otherwise acceptable normal background checks; in such an instance, Supplier shall pay for the additional background checks. Supplier will coordinate with the State and its employees to complete the necessary background checks and criminal history investigations. Should any employee or subcontractor of the Supplier who will be providing services under the Contract not be acceptable as a result of the background check or criminal history investigation, the Customer may require replacement of the employee or subcontractor in question and, if no suitable replacement is made within a reasonable time, terminate the purchase order or other payment mechanism associated with the project or service.

15 Patents and Copyrights

Without exception, a product or deliverable price shall include all royalties or costs owed by the Supplier to any third party arising from the use of a patent, intellectual property, copyright or other property right held by such third party. Should any third party threaten or make a claim that any portion of a product or service provided by Supplier under the Contract infringes that party's patent, intellectual property, copyright or other property right, Supplier shall enable each affected Customer to legally continue to use, or modify for use, the portion of the product or service at issue or replace such potentially infringing product, or re-perform or redeliver in the case of a service, with at least a functional non-infringing equivalent. Supplier's duty under this section shall extend to include any other product or service rendered materially unusable as intended due to replacement or modification of the product or service at issue. If the Supplier determines that none of these alternatives are reasonably available, the State shall return such portion of the product or deliverable at issue to the Supplier, upon written request, in exchange for a refund of the price paid for such returned goods as well as a refund or reimbursement, if applicable, of the cost of any other product or deliverable rendered materially unusable as intended due to removal of the portion of product or deliverable at issue. Any remedy provided under this section is not an exclusive remedy and is not intended to operate as a waiver of legal or equitable remedies because of acceptance of relief provided by Supplier.

16 Indemnification

16.1 State Shall Not Indemnify

The State of Oklahoma cannot lawfully agree to indemnify a private contractor. The credit of the State shall not be given, pledged, or loaned to any individual, company, corporation, or association, municipality, or political subdivision of the State pursuant to Oklahoma Constitution article 10, Section 15, OAC 260:115-7-32(k)(3)(A) and Attorney General Opinion 2012-18.

16.2 Acts or Omissions

A. Supplier shall defend and indemnify the Indemnified Parties, as applicable, for any and all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising out of, or resulting from any action or claim for bodily injury, death, or property damage brought against any of the Indemnified parties to the extent arising from any negligent act or omission or willful misconduct of the Supplier or its agents, employees, or subcontractors in the execution or performance of the Contract.

B. To the extent Supplier is found liable for loss, damage, or destruction of any property of Customer due to negligence, misconduct, wrongful act, or omission on the part of the Supplier, its employees, agents, representatives, or subcontractors, the Supplier and Customer shall use best efforts to mutually negotiate an equitable settlement amount to repair or replace the property unless such loss, damage or destruction is of such a magnitude that repair or replacement is not a reasonable option. Such amount shall be invoiced to, and is payable by Supplier sixty (60) calendar days after the date of Supplier's receipt of an invoice for the negotiated settlement amount.

16.3 Infringement

Supplier shall indemnify the Indemnified Parties, as applicable, for all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising from or in connection with Supplier's breach of its representations and warranties in the Contract or alleged infringement of any patent, intellectual property, copyright or other property right in connection with a product or service provided under the Contract. Supplier's duty under this section is reduced to the extent a claimed infringement results from: (a) a Customer's or user's content; (b) modifications by Customer or third party to a product delivered under the Contract or combinations of the product with any non-Supplier-provided services or products unless Supplier recommended or participated in such modification or combination; (c) use of a product or service by Customer in violation of the Contract unless done so at the direction of Supplier, or

(d) a non-Supplier product that has not been provided to the State by, through or on behalf of Supplier as opposed to its combination with products Supplier provides to or develops for the State or a Customer as a system.

16.4 Notice and Cooperation

In connection with indemnification obligations under the Contract, the parties agree to furnish prompt written notice to each other of any third-party claim. Any Customer affected by the claim will reasonably cooperate with Supplier and defense of the claim to the extent its interests are aligned with Supplier. Supplier shall use counsel reasonably experienced in the subject matter at issue and will not settle a claim without the written consent of the party being defended, which consent will not be unreasonably withheld or delayed, except that no consent will be required to settle a claim against Indemnified Parties that are not a State agency, where relief against the Indemnified Parties is limited to monetary damages that are paid by the defending party under indemnification provisions of the Contract.

16.5 Coordination of Defense

In connection with indemnification obligations under the Contract, when a State agency is a named defendant in any filed or threatened lawsuit, the defense of the State agency shall be coordinated by the Attorney General of Oklahoma, or the Attorney General may authorize the Supplier to control the defense and any related settlement negotiations; provided, however, Supplier shall not agree to any settlement of claims against the State without obtaining advance written concurrence from the Attorney General. If the Attorney General does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall have authorization to equally participate in any proceeding related to the indemnity obligation under the Contract and shall remain responsible to indemnify the applicable Indemnified Parties.

16.6 Limitation of Liability

A. With respect to any claim or cause of action arising under or related to the Contract, neither the State nor any Customer shall be liable to Supplier for lost profits, lost sales or business expenditures, investments, or commitments in connection with any business, loss of any goodwill, or for any other indirect, incidental, punitive, special or consequential damages, even if advised of the possibility of such damages.

B. Notwithstanding anything to the contrary in the Contract, no provision shall limit damages, expenses, costs, actions, claims, and liabilities arising from or related to property damage, bodily injury or death caused by Supplier or its employees, agents or subcontractors; indemnity, security or confidentiality obligations under the Contract; the bad faith, negligence, intentional misconduct or other acts for which applicable law does not allow exemption from liability of Supplier or its employees, agents or subcontractors.

C. The limitation of liability and disclaimers set forth in the Contract will apply regardless of whether Customer has accepted a product or service. The parties agree that Supplier has set its fees and entered into the Contract in reliance on the disclaimers and limitations set forth herein, that the same reflect an allocation of risk between the parties and form an essential basis of the bargain between the parties. These limitations shall apply notwithstanding any failure of essential purpose of any limited remedy.

17 Termination for Funding Insufficiency

17.1 Notwithstanding anything to the contrary in any Contract document, the State may terminate the Contract in whole or in part if funds sufficient to pay obligations under the Contract are not appropriated or received from an intended third-party funding source. In the event of such insufficiency, Supplier will be provided at least fifteen (15) calendar days' written notice of termination. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated. The determination by the State of insufficient funding shall be accepted by, and shall be final and binding on, the Supplier.

17.2 Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded.

17.3 The State's exercise of its right to terminate the Contract under this section shall not be considered a default or breach under the Contract or relieve the Supplier of any liability for claims arising under the Contract.

18 Termination for Cause

18.1 Supplier may terminate the Contract if (i) it has provided the State with written notice of material breach and (ii) the State fails to cure such material breach within thirty (30) days of receipt of written notice. If there is more than one Customer, material breach by a Customer does not give rise to a claim of material breach as grounds for termination by Supplier of the Contract as a whole. The State may terminate the Contract in whole or in part if (i) it has provided Supplier with written notice of material breach, and (ii) Supplier fails to cure such material breach within thirty (30) days of receipt of written notice. Any partial termination of the Contract under this section shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that are not terminated.

18.2 The State may terminate the Contract in whole or in part immediately without a thirty (30) day written notice to Supplier if (i) Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract; (ii) Supplier's material breach is reasonably determined to be an impediment to the function of the State and detrimental to the State or to cause a condition precluding the thirty (30) day notice or (iii) when the State determines that an administrative error in connection with award of the Contract occurred prior to Contract performance.

18.3 The State may terminate the Contract if the scope includes PR Vendor services and the Supplier, or Supplier's employee, violate the lobbying clause. PR Vendor services is defined to include a contract for public relations (PR), marketing or communication services. The State may immediately terminate the Contract with no more than 10-days notice under this section.

18.4 Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination is not an exclusive remedy but is in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

18.5 The Supplier's repeated failure to provide an acceptable product or service; Supplier's unilateral revision of linked or supplemental terms that have a materially adverse impact on a Customer's rights or obligations under the Contract (except as required by a governmental authority); actual or anticipated failure of Supplier to perform its obligations under the Contract; Supplier's inability to pay its debts when due; assignment for the benefit of Supplier's creditors; or voluntary or involuntary appointment of a receiver or filing of bankruptcy of Supplier shall constitute a material breach of the Supplier's obligations, which may result in partial or whole termination of the Contract. This subsection is not intended as an exhaustive list of material breach conditions. Termination may also result from other instances of failure to adhere to the Contract provisions and for other reasons provided for by applicable law, rules or regulations; without limitation, OAC 260:115-9-1 is an example.

19 Termination for Convenience

19.1 The State may terminate the Contract, in whole or in part, for convenience if it is determined that termination is in the State's best interest. In the event of a termination for convenience, Supplier will be provided at least thirty (30) days written notice of termination. Any partial termination of the Contract shall not be construed as a waiver of, and shall not affect, the rights and obligations of any party regarding portions of the Contract that remain in effect.

19.2 Upon receipt of notice of such termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory nor to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

20 Suspension of Supplier

20.1 Supplier may be subject to Suspension without advance notice and may additionally be suspended from activities under the Contract if Supplier fails to comply with confidentiality, privacy, security, environmental or safety requirements applicable to Supplier's performance or obligations under the Contract.

20.2 Upon receipt of a notice pursuant to this section, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to receipt of notice by Supplier, the Suspension does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract during a period of Suspension or suspended activity or for any damages or other amounts caused by or associated with such Suspension or suspended activity. A right exercised under this section shall not be an exclusive remedy but shall be in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees attributable to a period of Suspension or suspended activity shall be refunded.

20.3 Such Suspension may be removed, or suspended activity may resume, at the earlier of such time as a formal notice is issued that authorizes the resumption of performance under the Contract or at such time as a purchase order or other appropriate encumbrance document is issued. This subsection is not intended to operate as an affirmative statement that such a resumption will occur.

21 Certification Regarding Debarment, Suspension, and Other Responsibility Matters

The certification made by Supplier with respect to Debarment, Suspension, certain indictments, convictions, civil judgments and terminated public contracts is a material representation of fact upon which reliance was placed when entering into the Contract. A determination that Supplier knowingly rendered an erroneous certification, in addition to other available remedies, may result in whole or partial termination of the Contract for Supplier's default. Additionally, Supplier shall promptly provide written notice to the State Purchasing Director if the certification becomes erroneous due to changed circumstances.

22 Certification Regarding State Employees Prohibition From Fulfilling Services

Pursuant to 74 O.S. § 85.42, the Supplier certifies that no person involved in any manner in development of the Contract employed by the State shall be employed to fulfill any services provided under the Contract.

23 Force Majeure

23.1 Either party shall be temporarily excused from performance to the extent delayed as a result of unforeseen causes beyond its reasonable control including fire or other similar casualty, act of God, strike or labor dispute, war or other violence, or any law, order or requirement of any governmental agency or authority provided the party experiencing the force majeure event has prudently and promptly acted to take any and all steps within the party's control to ensure continued performance and to shorten duration of the event. If a party's performance of its obligations is materially hindered as a result of a force majeure event, such party shall promptly notify the other party of its best reasonable assessment of the nature and duration of the force majeure event and steps it is taking, and plans to take, to mitigate the effects of the force majeure event. The party shall use commercially reasonable best efforts to continue performance to the extent possible during such event and resume full performance as soon as reasonably practicable.

23.2 Subject to the conditions set forth above, non-performance as a result of a force majeure event shall not be deemed a default. However, a purchase order or other payment mechanism may be terminated if Supplier cannot cause delivery of a product or service in a timely manner to meet the business needs of Customer. Supplier is not entitled to payment for products or services not received and, therefore, amounts payable to Supplier during the force majeure event shall be equitably adjusted downward.

23.3 Notwithstanding the foregoing or any other provision in the Contract, (i) the following are not a force majeure event under the Contract: (a) shutdowns, disruptions or malfunctions in Supplier's system or any of Supplier's telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to Supplier's systems or (b) the delay or failure of Supplier or subcontractor personnel to perform any obligation of Supplier hereunder unless such delay or failure to perform is itself by reason of a force majeure event and (ii) no force majeure event modifies or excuses Supplier's obligations related to confidentiality, indemnification, data security or breach notification obligations set forth herein.

24 Security of Property and Personnel

In connection with Supplier's performance under the Contract, Supplier may have access to Customer personnel, premises, data, records, equipment and other property. Supplier shall use commercially reasonable best efforts to preserve the safety and security of such personnel, premises, data, records, equipment, and other property of Customer. Supplier shall be responsible for damage to such property to the extent such damage is caused by its employees or subcontractors and shall be responsible for loss of Customer property in its possession, regardless of cause. If Supplier fails to comply with Customer's security requirements, Supplier is subject to immediate suspension of work as well as termination of the associated purchase order or other payment mechanism.

25 Notices

All notices, approvals or requests allowed or required by the terms of any Contract document shall be in writing, reference the Contract with specificity and deemed delivered upon receipt or upon refusal of the intended party to accept receipt of the notice. In addition to other notice requirements in the Contract and the designated Supplier contact provided in a successful Bid, notices shall be sent to the State at the physical address set forth below. Notice information may be updated in writing to the other party as necessary. Notwithstanding any other provision of the Contract, confidentiality, breach and termination-related notices shall not be delivered solely via e-mail.

If Sent to the State:
State Purchasing Director
2401 N. Lincoln Blvd., Second Floor Oklahoma City, OK 73105

With a copy, which shall not constitute notice, to:
OMES Central Purchasing, Attn: Deputy General Counsel, 2401 N. Lincoln Blvd., Second Floor Oklahoma City, OK 73105

26 Miscellaneous

26.1 Choice of Law and Venue

Any claim, dispute, or litigation relating to the Contract documents, in the singular or in the aggregate, shall be governed by the laws of the State without regard to application of choice of law principles. Pursuant to 74 O.S. § 85.7(F), where federal granted funds are involved, applicable federal laws, rules and regulations shall govern to the extent necessary to insure benefit of such federal funds to the State. Venue for any action, claim, dispute, or litigation relating in any way to the Contract documents, shall be in Oklahoma County, Oklahoma. The State expressly declines any terms that minimize its rights under Oklahoma law, including but not limited to, Statutes of Limitations.

26.2 Employment Relationship

The Contract does not create an employment relationship. Individuals providing products or performing services pursuant to the Contract are not employees of the State or Customer and, accordingly are not eligible for any rights or benefits whatsoever accruing to such employees.

26.3 Transition Services

If transition services are needed at the time of Contract expiration or termination, Supplier shall provide such services on a month-to-month basis, at the contract rate or other mutually agreed rate. Supplier shall provide a proposed transition plan, upon request, and cooperate with any successor supplier and with establishing a mutually agreeable transition plan. Failure to cooperate may be documented as poor performance of Supplier.

26.4 Publicity

The existence of the Contract or any Acquisition is in no way an endorsement of Supplier, the products or services and shall not be so construed by Supplier in any advertising or publicity materials. Supplier agrees to submit to the State all advertising, sales, promotion, and other publicity matters relating to the Contract wherein the name of the State or any Customer is mentioned or language used from which, in the State's judgment, an endorsement may be inferred or implied. Supplier further agrees not to publish or use such advertising, sales promotion, or publicity matter or release any informational pamphlets, notices, press releases, research reports, or similar public notices concerning the Contract or any Acquisition hereunder without obtaining the prior written approval of the State.

26.5 Open Records Act

Supplier acknowledges that all State agencies and certain other Customers are subject to the Oklahoma Open Records Act set forth at 51 O.S. § 24A-1 et seq. Supplier also acknowledges that compliance with the Oklahoma Open Records Act and all opinions of the Oklahoma Attorney General concerning the Act is required. Nothing herein is intended to waive the State Purchasing Director's authority under OAC 260:115-3-9 in connection with Bid information requested to be held confidential by a Bidder. Notwithstanding the foregoing, Supplier Confidential Information shall not include information that: (i) is or becomes generally known or available by public disclosure, commercial use or otherwise and is not in contravention of this Contract; (ii) is known and has been reduced to tangible form by the receiving party before the time of disclosure for the first time under this Contract and without other obligations of confidentiality; (iii) is independently developed without the use of any of Supplier Confidential Information; (iv) is lawfully obtained from a third party (without any confidentiality obligation) who has the right to make such disclosure or (v) pricing provided to the State. In addition, the obligations in this section shall not apply to the extent that the applicable law or regulation requires disclosure of Supplier Confidential Information, provided that the Customer provides reasonable written notice, pursuant to Contract notice provisions, to the Supplier so that the Supplier may promptly seek a protective order or other appropriate remedy.

26.6 Failure to Enforce

Failure by the State or a Customer at any time to enforce a provision of, or exercise a right under, the Contract shall not be construed as a waiver of any such provision. Such failure to enforce or exercise shall not affect the validity of any Contract document, or any part thereof, or the right of the State or a Customer to enforce any provision of, or exercise any right under, the Contract at any time in accordance with its terms. Likewise, a waiver of a breach of any provision of a Contract document shall not affect or waive a subsequent breach of the same provision or a breach of any other provision in the Contract.

26.7 Mutual Responsibilities

A. No party to the Contract grants the other the right to use any trademarks, trade names, other designations in any promotion or publication without the express written consent by the other party.

B. The Contract is a non-exclusive contract and each party is free to enter into similar agreements with others.

C. The Customer and Supplier each grant the other only the licenses and rights specified in the Contract and all other rights and interests are expressly reserved.

D. The Customer and Supplier shall reasonably cooperate with each other and any Supplier to which the provision of a product and/or service under the Contract may be transitioned after termination or expiration of the Contract.

E. Except as otherwise set forth herein, where approval, acceptance, consent, or similar action by a party is required under the Contract, such action shall not be unreasonably delayed or withheld.

26.8 Invalid Term or Condition

To the extent any term or condition in the Contract conflicts with a compulsory applicable State or United States law or regulation, such Contract term or condition is void and unenforceable. By executing any Contract document which contains a conflicting term or condition, no representation or warranty is made regarding the enforceability of such term or condition. Likewise, any applicable State or federal law or regulation which conflicts with the Contract or any non-conflicting applicable State or federal law or regulation is not waived.

26.9 Severability

If any provision of a Contract document, or the application of any term or condition to any party or circumstances, is held invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable and the application of such provision to other parties or circumstances shall remain valid and in full force and effect. If a court finds that any provision of this contract is invalid or unenforceable, but that by limiting such provision it would become valid and enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited.

26.10 Section Headings

The headings used in any Contract document are for convenience only and do not constitute terms of the Contract.

26.11 Sovereign Immunity

Notwithstanding any provision in the Contract, the Contract is entered into subject to the State's Constitution, statutes, common law, regulations, and the doctrine of sovereign immunity, none of which are waived by the State nor any other right or defense available to the State.

26.12 Survival

As applicable, performance under all license, subscription, service agreements, statements of work, transition plans and other similar Contract documents entered into between the parties under the terms of the Contract shall survive Contract expiration. Additionally, rights and obligations under the Contract which by their nature should survive including, without limitation, certain payment obligations invoiced prior to expiration or termination; confidentiality obligations; security incident and data breach obligations and indemnification obligations, remain in effect after expiration or termination of the Contract.

26.13 Entire Agreement

The Contract documents taken together as a whole constitute the entire agreement between the parties. No statement, promise, condition, understanding, inducement or representation, oral or written, expressed or implied, which is not contained in a Contract document shall be binding or valid. The Supplier's representations and certifications, including any completed electronically, are incorporated by reference into the Contract.

26.14 Gratuities

The Contract may be immediately terminated, in whole or in part, by written notice if it is determined that the Supplier, its employee, agent, or another representative violated any federal, State or local law, rule or ordinance by offering or giving a gratuity to any State employee directly involved in the Contract. In addition, Suspension or Debarment of the Supplier may result from such a violation.

26.15 Import/Export Controls

Neither party will use, distribute, transfer or transmit any equipment, services, software or technical information provided under the Contract (even if incorporated into other products) except in compliance with all applicable import and export laws, conventions and regulations.

ATTACHMENT C

AGENCY TERMS

SOLICITATION NO. EV00000780

Intentionally left blank

ATTACHMENT D

STATE OF OKLAHOMA INFORMATION TECHNOLOGY TERMS

The parties further agree to the following terms ("Information Technology Terms"), as applicable, for any Acquisition of products or services with an information technology or telecommunication component. Pursuant to the Oklahoma Information Technology Consolidation and Coordination Act ("The Act" or "Act"), OMES- Information Services ("OMES-IS") is designated to purchase information technology and telecommunication products and services on behalf of the State. The Act directs OMES-IS to acquire necessary hardware, software and services and to authorize the use by other State agencies. OMES, as the owner of information technology and telecommunication assets and contracts on behalf of the State, allows other State agencies to use the assets while retaining ownership and the right to reassign the assets, at no additional cost, upon written notification to Supplier. OMES-IS is the data custodian for State agency data; however, such data is owned by the respective State agency.

1 DEFINITIONS

1.1 **Customer Data** means all data supplied by or on behalf of a Customer in connection with the Contract, excluding any confidential information of Supplier. Customer Data includes both Non-Public Data and Personal Data.

1.2 **Data Breach** means the unauthorized access or the reasonable suspicion of unauthorized access, by an unauthorized person that results in the use, destruction, loss, alteration, disclosure, or theft of Customer Data.

1.3 **Host** includes the terms Hosted or Hosting and means the accessing, processing or storing of Customer Data.

1.4 **Intellectual Property Rights** means the worldwide legal rights or interests evidenced by or embodied in any idea, design, concept, personality right, method, process, technique, apparatus, invention, discovery or improvement including any patents, trade secrets and know-how; any work of authorship including any copyrights, Moral Rights or neighboring rights; any trademark, service mark, trade dress, trade name or other indicia of source or origin; domain name registrations; and any other proprietary or similar rights. Intellectual Property Rights of a party also includes all worldwide legal rights or interests that the party may have acquired by assignment or license with the right to grant sublicenses.

1.5 **Non-Public Data** means Customer Data, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by Customer because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information. Non-Public Data includes any data deemed confidential pursuant to the Contract, otherwise identified by Customer as Non-Public Data, or that a reasonable person would deem confidential.

1.6 **Personal Data** means Customer Data that contains 1) any combination of an individual's name, social security numbers, driver's license, state/federal identification number, account number, credit or debit card number and/or 2) data subject to protection under a federal, state or local law, rule, regulation or ordinance.

1.7 **Security Incident** means the attempted or successful unauthorized access, use, disclosure, modification, loss, theft, or destruction of information or interference with the Hosted environment used to perform the services.

1.8 **Supplier** means the Bidder with whom the State enters into the Contract awarded pursuant to the Solicitation or the business entity or individual that is a party to the Contract with the State. A Supplier with whom the State enters into an awarded Contract shall also be known as a Contractor.

1.9 **Supplier Intellectual Property** means all tangible or intangible items or things, including the Intellectual Property Rights therein, created or developed by Supplier and identified in writing as such (a) prior to providing any services or Work Product to Customer and prior to receiving any documents, materials, information or funding from or on behalf of a Customer relating to the services or Work Product, or (b) after the effective date of the Contract if such tangible or intangible items or things were independently developed by Supplier outside Supplier's provision of services or Work Product for Customer under the Contract and were not created, prepared, developed, invented or conceived by any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

1.10 **Third Party Intellectual Property** means the Intellectual Property Rights of any third party that is not a party to the Contract, and that is not directly or indirectly providing any goods or services to a Customer under the Contract.

2 TERMINATION OF MAINTENANCE AND SUPPORT SERVICES

Customer may terminate maintenance or support services without an adjustment charge, provided any of the following circumstances occur:

2.1 Customer removes the product for which the services are provided, from productive use; or,

2.2 The location at which the services are provided is no longer controlled by Customer (for example, because of statutory or regulatory changes or the sale or closing of a facility).

2.3 If Customer chooses to renew maintenance or support after maintenance has lapsed, Customer may choose to pay the additional fee, if any, associated with renewing a license after such maintenance or support has lapsed, or to purchase a new license. Any amount paid to Supplier in the form of prepaid fees that are unused when services under the Contract or purchase order are terminated shall be refunded to Customer.

3 COMPLIANCE AND ELECTRONIC AND INFORMATION TECHNOLOGY ACCESSIBILITY

3.1 State procurement of information technology is subject to certain federal and State laws, rules and regulations related to information technology accessibility, including but not limited to Oklahoma Information Technology Accessibility Standards ("Standards") set forth at Information and Communication Technology Accessibility Standards (oklahoma.gov). Supplier shall provide a Voluntary Product Accessibility Template ("VPAT") describing accessibility compliance via a URL linking to the VPAT and shall update the VPAT as necessary in order to allow a Customer to obtain current VPAT information as required by State law. If products require development or customization, additional requirements and documentation may be required and compliance shall be necessary by Supplier. Such requirements may be stated in appropriate documents including but not limited to a statement of work, riders, agreement, purchase order or Addendum.

All representations contained in the VPAT provided will be relied upon by the State or a Customer, as applicable, for accessibility compliance purposes.

4 MEDIA OWNERSHIP (Disk Drive and/or Memory Chip Ownership)

4.1 Any disk drives and memory cards purchased with or included for use in leased or purchased products under the Contract remain the sole and exclusive property of the Customer.

4.2 Personal information may be retained within electronic media devices and components; therefore, electronic media shall not be released either between Customers or for the resale, of refurbished equipment that has been in use by a Customer, by the Supplier to the general public or other entities. This provision applies to replacement devices and components, whether purchased or leased, supplied by Supplier, its agents or subcontractors during the downtime (repair) of products purchased or leased through the Contract. If a device is removed from a location for repairs, the Customer shall have sole discretion, prior to removal, to determine and implement sufficient safeguards (such as a record of hard drive serial numbers) to protect personal information that may be stored within the hard drive or memory of the device.

5 OFFSHORE SERVICES

No offshore services are provided for under the Contract. State data shall not be used or accessed internationally for troubleshooting or any other use not specifically provided for herein without the prior written permission, which may be withheld in the State's sole discretion, from the appropriate authorized representative of the State. Notwithstanding the above, back office administrative functions of the Supplier may be located offshore and the follow-the-sun support model may be used by the Supplier to the extent allowed by law applicable to any Customer data being accessed or used.

6 COMPLIANCE WITH TECHNOLOGY POLICIES

6.1 The Supplier agrees to adhere to the State of Oklahoma "Information Security Policy, Procedures, and Guidelines" available at https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf.

Supplier's employees and subcontractors shall adhere to the applicable State IT

Standards, policies, procedures and architectures as set forth at https://oklahoma.gov/omes/services/information-services.html or as otherwise provided by the State.

6.2 Supplier shall comply with applicable Federal Information Processing Standards including, without limitation, FIPS 200, FIPS 140-2 or successor standards and all recommendations from the National Institute of Standards and Technology. The confidentiality of Customer Data shall be protected and maintained in accordance with these standards as well as other applicable Customer standards.

7 EMERGING TECHNOLOGIES

The State reserves the right to enter into an Addendum to the Contract at any time to allow for emerging technologies not identified elsewhere in the Contract documents if there are repeated requests for such emerging technology or the State determines it is warranted to add such technology.

8 EXTENSION RIGHT

In addition to extension rights of the State set forth in the Contract, the State Chief Information Officer reserves the right to extend any Contract at his or her sole option if the State Chief Information Officer determine such extension to be in the best interest of the State.

9 SOURCE CODE ESCROW

Pursuant to 62 O.S. § 34.31, if customized computer software is developed or modified exclusively for a State agency, the Supplier has a continuing obligation to comply with such law and place the source code for such software and any modifications thereto into escrow with an independent third-party escrow agent. Supplier shall pay all fees charged by the escrow agent and enter into an escrow agreement, the terms of which are subject to the prior written approval of the State, including terms that provide the State receives ownership of all escrowed source code upon the occurrence of any of the following:

9.1 A bona fide material default of the obligations of the Supplier under the agreement with the applicable Customer;

9.2 An assignment by the Supplier for the benefit of its creditors;

9.3 A failure by the Supplier to pay, or an admission by the Supplier of its inability to pay, its debts as they mature;

9.4 The filing of a petition in bankruptcy by or against the Supplier when such petition is not dismissed within sixty (60) days of the filing date;

9.5 The appointment of a receiver, liquidator or trustee appointed for any substantial part of the Supplier's property;

9.6 The inability or unwillingness of the Supplier to provide the maintenance and support services in accordance with the agreement with the agency;

9.7 Supplier's ceasing of maintenance and support of the software; or

9.8 Such other condition as may be statutorily imposed by the future amendment or enactment of applicable Oklahoma law.

10 COMMERCIAL OFF THE SHELF SOFTWARE OR SUPPLIER TERMS

If Supplier specifies terms and conditions or clauses in an electronic license, subscription, maintenance, support or similar agreement, including via a hyperlink or uniform resource locator address to a site on the internet, that conflict with the terms of this Contract, the additional terms and conditions or conflicting clauses shall not be binding on the State and the provisions of this Contract shall prevail. Further, no such terms and conditions or clauses shall expand the State's or Customer's liability or reduce the rights of Customer or the State.

11 OWNERSHIP RIGHTS

Any software developed, modified, or customized by the Supplier in accordance with a mutually negotiated statement of work pursuant to this Contract is for the sole and exclusive use of the State including but not limited to the right to use, reproduce, re-use, alter, modify, edit, or change the software as it sees fit and for any purpose. The parties mutually agree the State as a licensee of the Supplier does not make a claim of ownership to the existing Intellectual Property of Supplier. Moreover, except with regard to any deliverable based on Supplier Intellectual Property, the State shall be deemed the sole and exclusive owner of all right, title, and interest therein, including but not limited to all source data, information and materials furnished to the State, together with all plans, system analysis, and design specifications and drawings, completed programs and documentation thereof, reports and listing, all data and test procedures and all other items pertaining to the work and services to be performed pursuant to this Contract including all copyright and proprietary rights relating thereto. With respect to Supplier Intellectual Property, the Supplier grants the State, for no additional consideration, a perpetual, irrevocable, royalty-free license, solely for the internal business use of the State, to use, copy, modify, display, perform, transmit and prepare derivative works of Supplier Intellectual Property embodied in or delivered to the State in conjunction with the products.

Except for any Supplier Intellectual Property, all work performed by the Supplier of developing, modifying or customizing software and any related supporting documentation shall be considered as Work for Hire (as defined under the U.S. copyright laws) and, as such, shall be owned by and for the benefit of State.

In the event that it should be determined that any portion of such software or related supporting documentation does not qualify as "Work for Hire", Supplier hereby irrevocably grants to the State, for no additional consideration, a non-exclusive, irrevocable, royalty-free license to use, copy, modify, display, perform, transmit and prepare derivative works of any such software and any Supplier Intellectual Property embodied in or delivered to the State in conjunction with the products.

Supplier shall assist the State and its agents, upon request, in preparing U.S. and foreign copyright, trademark, and/or patent applications covering software developed, modified or customized for the State when made in accordance with a mutually negotiated statement of work pursuant to this Contract. Supplier shall sign any such applications, upon request, and deliver them to the State. The State shall bear all expenses that incurred in connection with such copyright, trademark, and/or patent applications.

If any Acquisition pursuant to this Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation owned by the State may be shared with other publicly funded agencies at the discretion of the State without permission from or additional compensation to the Supplier.

12 INTELLECTUAL PROPERTY OWNERSHIP TO WORK PRODUCT

The following terms apply to ownership and rights related to Intellectual Property:

12.1 As to the Intellectual Property Rights to Work Product between Supplier and Customer, Customer shall be the exclusive owner and not Supplier. Supplier specifically agrees that the Work Product shall be considered “works made for hire” and that the Work Product shall, upon creation, be owned exclusively by Customer. To the extent that the Work Product, under applicable law, may not be considered works made for hire, Supplier agrees that all right, title and interest in and to all ownership rights and all Intellectual Property Rights in the Work Product is effectively transferred, granted, conveyed, assigned, and relinquished exclusively to Customer, without the necessity of any further consideration, and Customer shall be entitled to obtain and hold in its own name all Intellectual Property Rights in and to the Work Product. Supplier acknowledges that Supplier and Customer do not intend Supplier to be a joint author of the Work Product within the meaning of the Copyright Act of 1976. Customer shall have access, during normal business hours (Monday through Friday, 8:00 a.m. to 5:00 p.m.) and upon reasonable prior notice to Supplier, to all Supplier materials, premises and computer files containing the Work Product. Supplier and Customer, as appropriate, will cooperate with one another and execute such other documents as may be reasonably appropriate to achieve the objectives herein. No license or other right is granted under the Contract to any Third-Party Intellectual Property, except as may be incorporated in the Work Product by Supplier.

12.2 Supplier, upon request and without further consideration, shall perform any acts that may be deemed reasonably necessary or desirable by Customer to evidence more fully the transfer of ownership and/or registration of all Intellectual Property Rights in all Work Product to Customer to the fullest extent possible including, but not limited to, the execution, acknowledgement and delivery of such further documents in a form determined by Customer. In the event Customer shall be unable to obtain Supplier’s signature due to the dissolution of Supplier or Supplier’s failure to respond to Customer’s repeated requests for such signature on any document reasonably necessary for any purpose set forth in the foregoing sentence, Supplier hereby irrevocably designates and appoints Customer and its duly authorized officers and agents as Supplier’s agent and Supplier’s attorney-in-fact to act for and in Supplier’s behalf and stead to execute and file any such document and to do all other lawfully permitted acts to further any such purpose with the same force and effect as if executed and delivered by Supplier, provided however that no such grant of right to Customer is applicable if Supplier fails to execute any document due to a good faith dispute by Supplier with respect to such document. It is understood that such power is coupled with an interest and is therefore irrevocable. Customer shall have the full and sole power to prosecute such applications and to take all other action concerning the Work Product, and Supplier shall cooperate, at Customer’s sole expense, in the preparation and prosecution of all such applications and in any legal actions and proceedings concerning the Work Product.

12.3 Supplier hereby irrevocably and forever waives, and agrees never to assert, any Moral Rights in or to the Work Product which Supplier may now have or which may accrue to Supplier's benefit under U.S. or foreign copyright or other laws and any and all other residual rights and benefits which arise under any other applicable law now in force or hereafter enacted. Supplier acknowledges the receipt of equitable compensation for its assignment and waiver of such Moral Rights.

12.4 All documents, information and materials forwarded to Supplier by Customer for use in and preparation of the Work Product shall be deemed the confidential information of Customer, subject to the license granted by Customer to Supplier hereunder. Supplier shall not otherwise use, disclose, or permit any third party to use or obtain the Work Product, or any portion thereof, in any manner without the prior written approval of Customer.

12.5 These provisions are intended to protect Customer's proprietary rights pertaining to the Work Product and the Intellectual Property Rights therein and any misuse of such rights would cause substantial and irreparable harm to Customer's business. Therefore, Supplier acknowledges and stipulates that a court of competent jurisdiction may immediately enjoin a material breach of the Supplier's obligations with respect to confidentiality provisions of the Contract and the Work Product and a Customer's Intellectual Property Rights, upon a request by Customer, without requiring proof of irreparable injury, as same is presumed.

12.6 Upon the request of Customer, but in any event upon termination or expiration of this Contract or a statement of work, Supplier shall surrender to Customer all documents and things pertaining to the Work Product, generated or developed by Supplier or furnished by Customer to Supplier, including all materials embodying the Work Product, any Customer confidential information and Intellectual Property Rights in such Work Product, regardless of whether complete or incomplete. This section is intended to apply to all Work Product as well as to all documents and things furnished to Supplier by Customer or by anyone else that pertains to the Work Product.

12.7 Customer hereby grants to Supplier a non-transferable, non-exclusive, royalty-free, fully paid license to use any Work Product solely as necessary to provide services to Customer. Except as provided in this section, neither Supplier nor any subcontractor shall have the right to use the Work Product in connection with the provision of services to its other customers without the prior written consent of Customer, which consent may be withheld in Customer's sole discretion.

12.8 To the extent that any Third Party Intellectual Property is embodied or reflected in the Work Product or is necessary to provide services, Supplier shall obtain from the applicable third party for the Customer's benefit, an irrevocable, perpetual, non-exclusive, worldwide, royalty-free license, solely for Customer's internal business purposes; likewise, with respect to any Supplier Intellectual Property embodied or reflected in the Work Product or necessary to provide services, Supplier grants to Customer an irrevocable, perpetual, non- exclusive, worldwide, royalty-free license, solely for the Customer's internal business purposes. Each such license shall allow the applicable Customer to (i) use, copy, modify, display, perform (by any means), transmit and prepare derivative works of any Third Party Intellectual Property or Supplier Intellectual Property embodied in or delivered to Customer in conjunction with the WorkProduct and (ii) authorize others to do any or all of the foregoing. Supplier agrees to notify Customer on delivery of the Work Product or services if such materials include any Third Party Intellectual Property. The foregoing license includes the right to sublicense third parties, solely for the purpose of engaging such third parties to assist or carry out Customer's internal business use of the Work Product. Except for the preceding license, all rights in Supplier Intellectual Property remain in Supplier. On request, Supplier shall provide Customer with documentation indicating a third party's written approval for Supplier to use any Third Party Intellectual Property that may be embodied or reflected in the Work Product.

12.9 Supplier agrees that it shall have written agreement(s) that are consistent with the provisions hereof related to Work Product and Intellectual Property Rights with any employees, agents, consultants, contractors or subcontractors providing services or Work Product pursuant to the Contract, prior to the provision of such services or Work Product and that it shall maintain such written agreements at all times during performance of this Contract which are sufficient to support all performance and grants of rights by Supplier. Copies of such agreements shall be provided to the Customer promptly upon request.

12.10 To the extent not inconsistent with Customer's rights in the Work Product or other provisions, nothing in this Contract shall preclude Supplier from developing for itself, or for others, materials which are competitive with those produced as a result of the services provided under the Contract, provided that no Work Product is utilized, and no Intellectual Property Rights of Customer therein are infringed by such competitive materials. To the extent that Supplier wishes to use the Work Product or acquire licensed rights in certain Intellectual Property Rights of Customer therein in order to offer competitive goods or services to third parties, Supplier and Customer agree to negotiate in good faith regarding an appropriate license and royalty agreement to allow for such.

12.11 If any Acquisition pursuant to the Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation and materials owned by a Customer may be shared with other publicly funded agencies at the discretion of such Customer without permission from or additional compensation to the Supplier.

13 HOSTING SERVICES

A Supplier shall be responsible for the obligations set forth in in this Contract, including those obligations related to breach reporting and associated costs when a Supplier Hosting Customer Data or providing products or services pursuant to an Acquisition, contributes to, or directly causes a Data Breach or a Security Incident. Likewise, Supplier shall be responsible for the obligations set forth in in this Contract, including those obligations related to breach reporting and associated costs when a Supplier's affiliate or subcontractor contributes to, or directly causes a Data Breach or a Security Incident.

14 CHANGE MANAGEMENT

When a scheduled change is made to products or services provided to a Customer that impacts the Customer's system related to such product or service, Supplier shall provide two (2) weeks' prior written notice of such change. When the change is an emergency change, Supplier shall provide twenty-four (24) hours' prior written notice of the change. Repeated failure to provide such notice may be an evaluation factor (as indicative of Supplier's past performance) upon renewal or if future bids submitted by Supplier are evaluated by the State.

15 SERVICE LEVEL DEFICIENCY

In addition to other terms of the Contract, in instances of the Supplier's repeated failure to provide an acceptable level of service or meet service level agreement metrics, service credits shall be provided by Supplier and may be used as an offset to payment due.

16 OWNERSHIP OF IT AND TELECOMMUNICATION ASSETS

Notwithstanding any other provision in the Contract and pursuant to the Oklahoma Information Technology Consolidation and Coordination Act, all information technology and telecommunication assets and contracts on behalf of appropriated agencies of the State belong to OMES-IS. OMES-IS allows other State agencies to use the assets while retaining ownership and the right to reassign the assets, at no additional cost, upon written notification to Supplier.

17 CUSTOMER DATA

17.1 The parties agree to the following provisions in connection with any Customer Data accessed, processed transmitted, or stored by or on behalf of the Supplier and the obligations, representations and warranties set forth below shall continue as long as the Supplier has an obligation under the Contract.

17.2 Customer will be responsible for the accuracy and completeness of all Customer Data provided to Supplier by Customer. Customer shall retain exclusive ownership of rights, title, and interest in Customer Data. Non-Public Data and Personal Data shall be deemed to be Customer's confidential information. Supplier shall restrict access to Customer Data to their employees with a need to know (and advise such employees of the confidentiality and non-disclosure obligations assumed herein).

17.3 Supplier shall promptly notify the Customer upon receipt of any requests from unauthorized third parties which in any way might reasonably require access to Customer Data or Customer's use of the Hosted environment. Supplier shall notify the Customer by the fastest means available and also in writing pursuant to Contract notice provisions and the notice provision herein. Except to the extent required by law, Supplier shall not respond to subpoenas, service or process, Freedom of Information Act or other open records requests, and other legal request related to Customer without first notifying the Customer and obtaining the Customer's prior approval, which shall not be unreasonably withheld, of Supplier's proposed responses. Supplier agrees to provide its completed responses to the Customer with adequate time for Customer review, revision and approval.

17.4 Supplier will use commercially reasonable efforts to prevent the loss of or damage to Customer Data in its possession and will maintain commercially reasonable back-up procedures and copies to facilitate the reconstruction of any Customer Data that may be lost or damaged by Supplier. Supplier will promptly notify Customer of any loss, damage to, or unauthorized access of Customer Data. Supplier will use commercially reasonable efforts to reconstruct any Customer Data that has been lost or damaged by Supplier as a result of its negligence or willful misconduct. If Customer Data is lost or damaged for reasons other than as a result of Supplier's negligence or willful misconduct, Supplier, at the Customer's expense, will, at the request of the State, use commercially reasonable efforts to reconstruct any Customer Data lost or damaged.

18 DATA SECURITY

18.1 Supplier will use commercially reasonable efforts, consistent with industry standards, to provide security for the Hosted environment and Customer Data and to protect against both unauthorized access to the Hosting environment, and unauthorized communications between the Hosting environment and the Customer's browser. Supplier shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind.

18.2 All Personal Data and Non-public Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of Personal Data. All Personal Data and Non-Public Data shall be subject to controlled access. Any stipulation of responsibilities shall be included in a Statement of Work and will identify specific roles and responsibilities.

18.3 Supplier represents and warrants to the Customer that the Hosting equipment and environment will be routinely checked with a commercially available, industry standard software application with up-to-date virus definitions. Supplier will regularly update the virus definitions to ensure that the definitions are as up-to-date as is commercially reasonable. Supplier will promptly purge all viruses discovered during virus checks. If there is a reasonable basis to believe that a virus may have been transmitted to Customer by Supplier, Supplier will promptly notify Customer of such possibility in a writing that states the nature of the virus, the date on which transmission may have occurred, and the means Supplier has used to remediate the virus. Should the virus propagate to Customer's IT infrastructure, Supplier is responsible for costs incurred by Customer for Customer to remediate the virus.

18.4 At no time shall any Customer Data or processes – that either belong to or are intended for the use of the State - be copied, disclosed, or retained by Supplier or any party related to Supplier for subsequent use in any transaction that does not include the State unless otherwise agreed to by the State.

18.5 Supplier shall provide its services to Customer and its users solely from data centers in the U.S. Storage of Customer Data at rest shall be located solely in data centers in the U.S. Supplier shall not allow its personnel or contractors to store Customer Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. Supplier shall permit its personnel and contractors to access Customer Data remotely only as required to fulfill Supplier's obligations under the Contract.

18.6 Supplier shall allow the Customer to audit conformance to the Contract terms. The Customer may perform this audit or contract with a third party at its discretion and at Customer's expense.

18.7 Supplier shall perform an independent audit of its data centers at least annually at its expense and provide a redacted version of the audit report upon request. Supplier may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

18.8 Any remedies provided are not exclusive and are in addition to other rights and remedies available under the terms of the Contract, at law or in equity.

19 SECURITY ASSESSMENT

19.1 The State requires any entity or third-party Supplier Hosting Oklahoma Customer Data to submit to a State Certification and Accreditation Review process to assess initial security risk. Supplier submitted to the review and met the State's minimum-security standards at time the Contract was executed. Failure to maintain the State's minimum-security standards during the term of the contract, including renewals, constitutes a material breach. Upon request, the Supplier shall provide updated data security information in connection with a potential renewal. If information provided in the security risk assessment changes, Supplier shall promptly notify the State and include in such notification the updated information; provided, however, Supplier shall make no change that results in lessened data protection or increased data security risk. Failure to provide the notice required by this section or maintain the level of security required in the Contract constitutes a material breach by Supplier and may result in a whole or partial termination of the Contract.

19.2 Any Hosting entity change must be approved in writing prior to such change. To the extent Supplier requests a different sub-contractor than the third-party Hosting Supplier already approved by the State, the different sub-contractor is subject to the State's approval. Supplier agrees not to migrate State's data or otherwise utilize the different third-party Hosting Supplier in connection with key business functions that are Supplier's obligations under the contract until the State approves the third-party Hosting Supplier's State Certification and Accreditation Review, which approval shall not be unreasonably withheld or delayed. In the event the third-party Hosting Supplier does not meet the State's requirements under the State Certification and Accreditation Review, Supplier acknowledges and agrees it will not utilize the third-party Supplier in connection with key business functions that are Supplier's obligations under the contract, until such third party meets such requirements.

20 SECURITY INCIDENT OR DATA BREACH NOTIFICATION

20.1 Supplier shall inform Customer of any Security Incident or Data Breach.

20.2 Supplier may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Contract. If a Security Incident involves Customer Data, Supplier will coordinate with Customer prior to any such communication.

20.3 Supplier shall report a Security Incident to the Customer identified contact set forth herein within five (5) days of discovery of the Security Incident or within a shorter notice period required by applicable law or regulation (i.e., HIPAA requires notice to be provided within 24 hours).

20.4 Supplier shall maintain processes and procedures to identify, respond to and analyze Security Incidents; (ii) make summary information regarding such procedures available to Customer at Customer's request, (iii) mitigate, to the extent practicable, harmful effects of Security Incidents that are known to Vendor; and (iv) documents all Security Incidents and their outcomes.

20.5 If Supplier has reasonable belief or actual knowledge of a Data Breach, Supplier shall (1) promptly notify the appropriate Customer identified contact set forth herein within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.

21 DATA BREACH NOTIFICATION AND RESPONSIBILITIES

This section only applies when a Data Breach occurs with respect to Personal Data or Non-Public Data within the possession or control of Supplier.

21.1 Supplier shall (1) cooperate with Customer as reasonably requested by Customer to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

21.2 Unless otherwise stipulated, if a Data Breach is a direct result of Supplier's breach of its obligation to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Supplier shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by state law; (3) credit monitoring services required by state or federal law; (4) a website or toll-free numbers and call center for affected individuals required by state law – all not to exceed the agency per record per person cost calculated for data breaches in the United States on the most recent Cost of Data breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Supplier based on root cause.

21.3 If a Data Breach is a direct result of Supplier's breach of its obligations to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Supplier shall indemnify and hold harmless the Customer against all penalties assessed to Indemnified Parties by governmental authorities in connection with the Data Breach.

22 SUPPLIER REPRESENTATIONS AND WARRANTIES

Supplier represents and warrants the following:

22.1 The product and services provided in connection with Hosting services do not infringe a third party's patent or copyright or other intellectual property rights.

22.2 Supplier will protect Customer's Non-Public Data and Personal Data from unauthorized dissemination and use with the same degree of care that each such party uses to protect its own confidential information and, in any event, will use no less than a reasonable degree of care in protecting such confidential information.

22.3 The execution, delivery and performance of the Contract and any ancillary documents and the consummation of the transactions contemplated by the Contract or any ancillary documents by Supplier will not violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third parties retained or utilized by Supplier to provide goods or services for the benefit of the Customer.

22.4 Supplier shall not knowingly upload, store, post, e-mail or otherwise transmit, distribute, publish or disseminate to or though the Hosting environment any material that contains software viruses, malware or other surreptitious code designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or circumvent any "copy-protected" devices, or any other harmful or disruptive program.

23 INDEMNITY

Supplier agrees to defend, indemnify and hold the State, its officers, directors, employees, and agents harmless from all liabilities, claims, damages, losses, costs, expenses, demands, suits and actions (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification), excluding damages that are the sole fault of Customer, arising from or in connection with Supplier's breach of its express representations and warranties in these Information Technology Terms and the Contract. If a third party claims that any portion of the products or services provided by Supplier under the terms of another Contract document or these Information Technology Terms infringes that party's patent or copyright, Supplier shall defend, indemnify and hold harmless the State and Customer against the claim at Supplier's expense and pay all related costs, damages, and attorney's fees incurred by or assessed to, the State and/or Customer. The State and/or Customer shall promptly notify Supplier of any third-party claims and to the extent authorized by the Attorney General of the State, allow Supplier to control the defense and any related settlement negotiations. If the Attorney General of the State does not authorize sole control of the defense and settlement negotiations to Supplier, Supplier shall be granted authorization to equally participate in any proceeding related to this section, but Supplier shall remain responsible to indemnify Customer and the State for all associated costs, damages and fees incurred by or assessed to the State and/or Customer. Should the software become, or in Supplier's opinion, be likely to become the subject of a claim or an injunction preventing its use as contemplated in connection with Hosting services, Supplier may, at its option (i) procure for the State the right to continue using the software or (ii) replace or modify the software with a like or similar product so that it becomes non-infringing.

24 TERMINATION, EXPIRATION AND SUSPENSION OF SERVICE

24.1 During any period of service suspension, Supplier shall not take any action to intentionally disclose, alter or erase any Customer Data.

24.2 In the event of a termination or expiration of the Contract, the parties further agree:

Supplier shall implement an orderly return of Customer Data in a format specified by the Customer and, as determined by the Customer:

a. return the Customer Data to Customer at no additional cost, at a time agreed to by the parties and the subsequent secure disposal of State Data;

b. transitioned to a different Supplier at a mutually agreed cost and in accordance with a mutually agreed data transition plan and the subsequent secure disposal of State Data or

c. a combination of the two immediately preceding options.

24.3 Supplier shall not take any action to intentionally erase any Customer Data for a period of:

a. 10 days after the effective date of termination, if the termination is in accordance with the contract period;

b. 30 days after the effective date of termination, if the termination is for convenience; or

c. 60 days after the effective date of termination if the termination is for cause.

After such period, Supplier shall, unless legally prohibited or otherwise stipulated, delete all Customer Data in its systems or otherwise in its possession or under its control.

24.4 The State shall be entitled to any post termination or expiration assistance generally made available with respect to the services.

24.5 Disposal by Supplier of Customer Data in all of its forms, such as disk, CD/DVD, backup tape and paper, when requested by the Customer, shall be performed in a secure manner. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to Customer within thirty (30) calendar day of its request for disposal of data.

25 GENERAL INFORMATION SECURITY REQUIREMENTS

25.1 No employee of Contractor or its subcontractors will be granted access to State of Oklahoma agency information systems without the prior completion and approval of applicable logon authorization and acceptable use requests.

25.2 Contractor or its subcontractors will notify applicable State of Oklahoma agencies when employees who have access to agency information systems are terminated.

25.3 Contractor or its subcontractors will disclose to Client any suspected breach of the security of the information system or the data contained therein in the most expedient time possible and without unreasonable delay and will cooperate with Client during the investigation of any such incident.

25.4 Contractor or its subcontractors agree to adhere to the State of Oklahoma "Information Security Policy, Procedures, and Guidelines" available at: https://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.pdf

26 HIPAA REQUIREMENTS

26.1 Contractor shall agree to use and disclose Protected Health Information in its possession or control in compliance with the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) (45 C.F.R. Parts 160 and 164) under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The definitions set forth in the Privacy Rule are incorporated by reference into this Contract (45 C.F.R. §§ 160.103 and 164.501).

26.2 If applicable, Contractor will sign and adhere to a Business Associate Agreement (BAA). The Business Associate Agreement provides for satisfactory assurances that Contractor will use the information only for the purposes for which it was engaged. Contractor agrees it will safeguard the information from misuse and will comply with HIPAA as it pertains to the duties stated within the contract. Failure to comply with the requirements of this standard may result in funding being withheld from Contractor, and/or full audit and inspection of Contractor's security compliance as it pertains to this contract.

26.3 Business Associate Terms Definitions:

a. Unless otherwise defined in this BAA, all capitalized terms used in this BAA have the meanings ascribed in the HIPAA Regulations, provided; however, that "PHI" and "ePHI" shall mean Protected Health Information and Electronic Protected Health Information, respectively, as defined in 45 C.F.R. § 160.103, limited to the information Business Associate received from or created or received on behalf of the applicable State of Oklahoma agency as a Business Associate. "Administrative Safeguards" shall have the same meaning as the term "administrative safeguards in 45 C.F.R. § 164.304, with the exception that it shall apply to the management of the conduct of Business Associate's workforce, not the State of Oklahoma agency workforce, in relation to the protection of that information.

b. Business Associate. "Business Associate" shall generally have the same meaning as the term "Business Associate" at 45 C.F.R. 160.103, and in reference to the party to this agreement, shall mean the entity whose name appears below.

c. Covered Entity. "Covered Entity" shall generally have the same meaning as the term "Covered Entity" at 45 C.F.R. 160.103.

d. HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164, all as may be amended.

e. The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, required by law, Secretary, Security Incident, Sub-Contractor, Unsecured PHI, and Use.

26.4 Obligations of Business Associate: Business Associate may use Electronic PHI and PHI (collectively, "PHI") solely to perform its duties and responsibilities under this Agreement and only as provided in this Agreement. Business Associate acknowledges and agrees that PHI is confidential and shall not be used or disclosed, in whole or in part, except as provided in this Agreement or as required by law. Specifically, Business Associate agrees it will, as applicable:

a. use or further disclose PHI only as permitted in this Agreement or as Required by Law, including, but not limited to the Privacy and Security Rule;

b. use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to Electronic PHI, to prevent use or disclosure of PHI other than as provided for by this Agreement;

c. implement and document appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of PHI that it creates, receives, maintains, or transmits for or on behalf of Covered Entity in accordance with 45 C.F.R. 164;

d. implement and document administrative safeguards to prevent, detect, contain, and correct security violations in accordance with 45 C.F.R. 164;

e. make its applicable policies and procedures required by the Security Rule available to Covered Entity solely for purposes of verifying BA's compliance and the Secretary of the Department of Health and Human Services (HHS);

f. not receive remuneration from a third party in exchange for disclosing PHI received from or on behalf of Covered Entity;

g. in accordance with 45 C.F.R. 164.502(e)(1) and 164.308(b), if applicable, require that any Sub-Contractors that create, receive, maintain or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information; this shall be in the form of a written HIPAA Business Associate Contract and a fully executed copy will be provided to the Contract Monitor;

h. report to Covered Entity in writing any use or disclosure of PHI that is not permitted under this Agreement as soon as reasonably practicable but in no event later than five calendar days from becoming aware of it and mitigate, to the extent practicable and in cooperation with Covered Entity, any harmful effects known to it of a use or disclosure made in violation of this Agreement;

i. promptly report to Covered Entity in writing and without unreasonable delay and in no case later than five calendar days any successful Security Incident, as defined in the Security Rule, with respect to Electronic PHI;

j. with the exception of law enforcement delays that satisfy the requirements of 45 C.F.R. 164.412, notify Covered Entity promptly, in writing and without unreasonable delay and in no case later than five calendar days, upon the discovery of a breach of Unsecured PHI. Such notice shall include, to the extent possible, the name of each individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such Breach. Business Associate shall also, to the extent possible, furnish Covered Entity with any other available information that Covered Entity is required to include in its notification to Individuals under 45 C.F.R. § 164.404(c) at the time of Business Associate's notification to Covered Entity or promptly thereafter as such information becomes available. As used in this Section, "breach" shall have the meaning given such term at 45 C.F.R. 164.402;

k. to the extent allowed by law, indemnify and hold Covered Entity harmless from all claims, liabilities costs, and damages arising out of or in any manner related to the unauthorized disclosure by Business Associate of any PHI resulting from the negligent acts or omissions of Business Associate or to the breach by Business Associate of any applicable obligation related to PHI;

l. provide access to PHI it maintains in a Designated Record Set to Covered Entity, or if directed by Covered Entity to an Individual in order to meet the requirements of 45 C.F.R. 164.524. In the event that any Individual requests access to PHI directly from Business Associate, Business Associate shall forward such request to Covered Entity within five working days of receiving a request. This shall be in the form of a written HIPAA Business Associate Contract and a fully executed copy will be provided to the Contract Monitor. Any denials of access to the PHI requested shall be the responsibility of Covered Entity;

m. make PHI it maintains in a Designated Record Set available to Covered Entity for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. 164.526;

n. document disclosure of PHI it maintains in a Designated Record Set and information related to such disclosure as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI, in accordance with 45 C.F.R. 164.528, and within five working days of receiving a request from Covered Entity, make such disclosure documentation and information available to Covered Entity. In the event the request for an accounting is delivered directly to Business Associate, Business Associate shall forward within five working days of receiving a request such request to Covered Entity;

o. make its internal practices, books, and records related to the use and disclosure of PHI received from or created or received by Business Associate on behalf of Covered Entity available to the Secretary of the Department of HHS, authorized governmental officials, and Covered entity for the purpose of determining Business Associate's compliance with the Privacy Rule. Business Associate shall give Covered Entity advance written notice of requests from HHS or government officials and provide Covered Entity with a copy of all documents made available; and

p. require that all of its Sub-Contractors, vendors, and agents to whom it provides PHI or who create, receive, use, disclose, maintain, or have access to Covered Entity's PHI shall agree in writing to requirements, restrictions, and conditions at least as stringent as those that apply to Business Associate under this Agreement, including but not limited to implementing reasonable and appropriate safeguards to protect PHI, and shall require that its Sub-Contractors, vendors, and agents agree to indemnify and hold harmless Covered Entity for their failure to comply with each of the provisions of this Agreement.

26.5 Permitted Uses and Disclosures of PHI by Business Associate: Except as otherwise provided in this Agreement, Business Associate may use or disclose PHI on behalf of or to provide services to Covered Entity for the purposes specified in this Agreement, if such use or disclosure of PHI would not violate the Privacy Rule if done by Covered Entity. Unless otherwise limited herein, Business Associate may:

a. use PHI for its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate;

b. disclose PHI for its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate, provided that; (i) the disclosures required by law; or (ii) Business Associate obtains reasonable assurances from any person to whom the PHI is disclosed that such PHI will be kept confidential and will be used or further disclosed only as Required by Law or for the purpose(s) for which it was disclosed to the person, and the person commits to notifying Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached;

c. disclose PHI to report violations of law to appropriate federal and state authorities; or

d. aggregate the PHI with other data in its possession for purposes of Covered Entity's Health Care Operations;

e. make uses and disclosures and requests for protected health information consistent with Covered Entity's minimum necessary policies and procedures;

f. de-identify any and all PHI obtained by Business Associate under this BAA, and use such de-identified data, all in accordance with the de-identification requirements of the Privacy Rule [45 C.F.R. § 164.502(d)].

26.6 Obligations of Covered Entity

a. Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

b. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 C.F.R. 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information.

c. Covered Entity shall not request Business Associate use or disclose PHI in any manner that would violate the Privacy Rule if done by Covered Entity.

d. Covered Entity agrees to timely notify Business Associate, in writing, of any arrangements between Covered Entity and the Individual that is the subject of PHI that may impact in any manner the use and/or disclosure of the PHI by Business Associate under this BAA.

e. Covered Entity shall provide the minimum necessary PHI to Business Associate.

26.7 Term and Termination:

a. Obligations of Business Associate upon Termination. Upon termination of this Agreement for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall as applicable:

i. retain only that PHI that is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

ii. return to Covered Entity (or, if agreed to by Covered Entity, destroy) the remaining PHI that the Business Associate still maintains in any form;

iii. continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;

iv. not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out at above under "Permitted Uses and Disclosures By Business Associate" that applied prior to termination; and

v. return to Covered Entity (or, if agreed to by Covered Entity, destroy) the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

b. All other applicable obligations of Business Associate under this Agreement shall survive termination.

c. Should the applicable State of Oklahoma agency become aware of a pattern of activity or practice that constitutes a material breach of a material term of this BAA by Business Associate, the agency shall provide Business Associate with written notice of such a breach in sufficient detail to enable Contractor to understand the specific nature of the breach. The Client shall be entitled to terminate the Underlying Contract associated with such breach if, after the applicable State of Oklahoma agency provides the notice to Business Associate, Business Associate fails to cure the breach within a reasonable time period not less than thirty (30) days specified in such notice; provided, however, that such time period specified shall be based on the nature of the breach involved per 45 C.F.R. §§ 164.504(e)(1)(ii)-(iii) & 164.314 (a)(2)(i)(C).

26.8 Miscellaneous Provisions:

a. No Third-Party Beneficiaries: Nothing in this Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

b. Business Associate recognizes that any material breach of this Business Associate Terms section or breach of confidentiality or misuse of PHI may result in the termination of this Agreement and/or legal action. Said termination may be immediate and need not comply with any termination provision in the parties' underlying agreement, if any.

c. The parties agree to amend this Agreement from time to time as is necessary for Covered Entity or Business Associate to comply with the requirements of the Privacy Rule and related laws and regulations.

d. The applicable State of Oklahoma agency shall make available its Notice of Privacy Practices.

e. Any ambiguity in this Agreement shall be resolved in a manner that causes this Agreement to comply with HIPAA.

f. If Business Associate maintains a designated record set in an electronic format on behalf of Covered Entity, then Business Associate agrees that within 30 calendar days of expiration or termination of the parties' agreement, Business Associate shall provide to Covered Entity a complete report of all disclosures of and access to the designated record set covering the three years immediately preceding the termination or expiration. The report shall include patient name, date and time of disclosures/access, description of what was disclosed/accessed, purpose of disclosure/access, name of individual who received or accessed the information, and, if available, what action was taken within the designated record set.

g. Amendment: To the extent that any relevant provision of the HIPAA Regulations is materially amended in a manner that changes the obligations of Business Associates or Covered Entities, the Parties agree to negotiate in good faith appropriate amendment(s) to this Agreement to give effect to these revised obligations. The parties agree to amend this Agreement from time to time as is necessary for Covered Entity or to comply with the requirements of the Privacy Rule and related laws and regulations.

27 42 C.F.R. PART 2 RELATED PROVISIONS

27.1 Confidentiality of Information. Contractor's employees and agents shall have access to private data to the extent necessary to carry out the responsibilities, limited by the terms of this Agreement. Contractor accepts the responsibilities for providing adequate administrative supervision and training to their employees and agents to ensure compliance with relevant confidentiality, privacy laws, regulations and contractual provisions. No private or confidential data collected, maintained, or used shall be disseminated except as authorized by statute and by terms of this Agreement, whether during the period of the Agreement or thereafter. Furthermore, Contractor:

27.2 Acknowledges that in receiving, transmitting, transporting, storing, processing, or otherwise dealing with any information received pursuant to this agreement that identifies or otherwise relates to the individuals under the care of or in the custody of a State of Oklahoma agency, it is fully bound by the provisions of the federal regulations governing the confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2 and the HIPAA, 45 C.F.R. 45 Parts 142, 160, and 164, Title 43 A § 1-109 of Oklahoma Statutes, and may not use or disclose the information except as permitted or required by this Agreement or by law;

27.3 Acknowledges that pursuant to 43A O.S. §1-109, all mental health and drug or alcohol treatment information and all communications between physician or psychotherapist and patient are both privileged and confidential and that such information is available only to persons actively engaged in treatment of the client or consumer or in related administrative work. Contractor agrees that such protected information shall not be available or accessible to staff in general and shall not be used for punishment or prosecution of any kind;

27.4 Agrees to resist any efforts in judicial proceedings to obtain access to the protected information except as expressly provided for in the regulations governing the Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2;

27.5 Agrees to, when applicable and to the extent within Contractor's control, use appropriate administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the State of Oklahoma agency and to use appropriate safeguards to prevent the unauthorized use or disclosure of the protected health information, and agrees that protected information will not be placed in the Child Protective Services (CPS) record of any individual involved with the Oklahoma Department of Human Services (DHS).

27.6 Agrees to report to the State of Oklahoma agency any use or disclosure or any security incident involving protected information not provided for by this Agreement. Such a report shall be made immediately when an employee becomes aware of such a disclosure, use, or security incident.

27.7 Agrees to provide access to the protected information at the request of the State of Oklahoma agency or to an authorized individual as directed by the State of Oklahoma agency, in order to meet the requirement of 45 C.F.R. §164.524 which provides clients with the right to access and copy their own protected information;

27.8 Agrees to make any amendments to the protected information as directed or agreed to by the State of Oklahoma agency, pursuant to 45 C.F.R. §164.526;

27.9 Agrees to make available its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of protected information received from the

State of Oklahoma agency or created or received by the Contractor on behalf of the State of Oklahoma agency, to the State of Oklahoma agency and to the Secretary of the Department of Health and Human Services for purpose of the Secretary determining the giving party's compliance with HIPAA;

27.10 Agrees to provide the State of Oklahoma agency, or an authorized individual, information to permit the State of Oklahoma agency to respond to a request by an individual for an accounting of disclosures in accordance with 45 C.F.R. §164.528.

28 DATA SECURITY

The Contractor agrees to, when applicable and to the extent within Contractor's control, maintain the data in a secure manner compatible with the content and use. The Contractor will, when applicable to the extent within Contractor's control, control access to the data in Contractor's possession or control compliance with the terms of this Agreement. Only the Contractor's personnel whose duties require the use of such information, will have regular access to the data. The Contractor's employees will be allowed access to the data only for the purpose set forth in this Agreement.

28.1 Data Destruction. Contractor agrees to, when applicable and to the extent within Contractor's control, follow State of Oklahoma agency policies regarding secure data destruction.

28.2 Use of Information. Contractor agrees that the information received or accessed through this Agreement shall not be used to the detriment of any individual nor for any purpose other than those stated in this Agreement.

28.3 Redisclosure of Data. The Contractor agrees not to redisclose any information to a third party not covered by the Agreement unless written permission by the State of Oklahoma agency is received and redisclosure is permitted under applicable law.

29 FEDERAL TAX INFORMATION REQUIREMENTS IRS PUBLICATION 1075

29.1 PERFORMANCE: If Contractor takes possession or control of Federal Tax Information in performance of this contract, the Contractor agrees to, when applicable and to the extent within Contractor's control, comply with and assume responsibility for compliance by officers or employees with the following requirements:

29.2 All work will be performed under the supervision of the State of Oklahoma.

29.3 The contractor and contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.

29.4 FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.

29.5 FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.

29.6 The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.

29.7 Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.

29.8 All Contractor computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

29.9 No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.

29.10 Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.

29.11 To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities which the contractor assumes toward the agency under this contract.

29.12 In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to the agency under this contract.

29.13 For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.

29.14 The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

30 CRIMINAL/CIVIL SANCTIONS

30.1 Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.

30.2 Each officer or employee of a contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

30.3 Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

30.4 Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

30.5 Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands the agency’s security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency’s security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see IRS Publication 1075, Exhibit 4, Sanctions for Unauthorized Disclosure, and IRS Publication 1075, Exhibit 5, Civil Damages for Unauthorized Disclosure). The training on the agency’s security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

31 INSPECTION

The IRS and the Agency, with 24-hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with FTI safeguard requirements.

32 SSA REQUIREMENTS

32.1 PERFORMANCE: If Contractor takes possession or control of in SSA provided information in the performance of this contract, the contractor agrees to, where applicable and to the extent within Contractor's control comply with and assume responsibility for compliance by his or her employees with the following requirements:

32.2 All work will be done under the supervision of the State of Oklahoma.

32.3 Any SSA provided information made available shall be used only for carrying out the provisions of this Agreement. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the Contractor is prohibited.

32.4 All SSA provided information shall be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.

32.5 No work involving SSA provided information furnished under this contract shall be subcontracted without prior written approval by the applicable State of Oklahoma agency and the SSA.

32.6 The Contractor shall maintain a list of employees authorized access. Such list shall be provided upon request to the applicable State of Oklahoma agency or the SSA.

32.7 Contractor or agents may not legally process, transmit, or store SSA-provided information in a cloud environment without explicit permission from SSA's Chief Information Officer. Proof of this authorization shall be provided to the Contractor by the applicable State of Oklahoma agency prior to accessing SSA provided information.

32.8 Contractor shall provide security awareness training to all employees, contractors, and agents who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training. Contractor is also required to certify that each employee, contractor, and agent who views SSA-provided information certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful assess and/or disclosure.

32.9 Contractor shall require employees, contractors, and agents to sign a non-disclosure agreement, attest to their receipt of Security Awareness Training, and acknowledge the rules of behavior concerning proper use and security in systems that process SSA-provided information. Contractor shall retain non-disclosure attestations for at least five (5) to seven (7) years for each employee who processes, views, or encounters SSA-provided information as part of their duties.

32.10 The applicable State of Oklahoma agency shall provide the Contractor a copy of the SSA exchange agreement and all related attachments before initial disclosure of SSA data. Contractor is required to follow the terms of the applicable State of Oklahoma agency's data exchange agreement with the SSA. Prior to signing this Agreement, and thereafter at SSA's request, the applicable State of Oklahoma agency shall obtain from the Contractor a current list of the employees of such Contractor with access to SSA data and provide such list to the SSA.

32.11 Where the Contractor processes, handles, or transmits information provided to the applicable State of Oklahoma agency by SSA or has authority to perform on the agency's behalf, the applicable State of Oklahoma agency shall clearly state the specific roles and functions of the Contractor within the Agreement.

32.12 SSA requires all parties subject to this Agreement to exercise due diligence to avoid hindering legal actions, warrants, subpoenas, court actions, court judgments, state or Federal investigations, and SSA special inquiries for matters pertaining to SSA-provided information.

32.13 SSA requires all parties subject to this Agreement to agree that any Client-owned or subcontracted facility involved in the receipt, processing, storage, or disposal of SSA-provided information operate as a "de facto" extension of the Client and is subject to onsite inspection and review by the Client or SSA with prior notice.

32.14 If the Contractor must send a Contractor computer, hard drive, or other computing or storage device offsite for repair, the Contractor must have a non-disclosure clause in their contract with the vendor. If the Contractor used the item in a business process that involved SSA-provided information and the vendor will retrieve or may view SSA-provided information during servicing, SSA reserves the right to inspect the Contractor's vendor contract. The Contractor must remove SSA-provided information from electronic devices before sending it to an external vendor for service. SSA expects the Contractor to render SSA-provided information unrecoverable or destroy the electronic device if they do not need to recover the information. The same applies to excessed, donated, or sold equipment placed into the custody of another organization.

32.15 In the event of a suspected or verified data breach involving SSA provided information, the Contractor shall notify the Client immediately.

32.16 The Client shall have the right to void the contract if the contractor fails to provide the safeguards described above.

33 CRIMINAL/CIVIL SANCTIONS

The Act specifically provides civil remedies, 5 U.S.C. Sec. 552a(g), including damages, and criminal penalties, 5 U.S.C. Sec. 552a(i), for violations of the Act. The civil action provisions are premised violations of the Act committed by parties subject to this Agreement or regulations promulgated thereunder. An individual claiming such a violation by parties subject to this Agreement may bring civil action in a federal district court. If the individual substantially prevails, the court may assess reasonable attorney fees and other litigation costs. In addition, the court may direct the parties subject to this Agreement to grant the plaintiff access to his/her records, and when appropriate direct an amendment or correction of records subject to the Act. Actual damages may be awarded to the plaintiff for intentional or willful refusal by parties subject to this Agreement to comply with the Act.

33.1 Civil Remedies

a. In any suit brought under the provisions of 5 U.S.C. § 552a(g)(1)(C) or (D) in which the court determines that the parties subject to this Agreement acted in a manner which was intentional or willful, shall be liable in an amount equal to the sum of

b. actual damages sustained by the individual because of the refusal or failure, but in no case, shall a person entitled to recovery receive less than the sum of $1,000; and

c. the costs of the action together with reasonable attorney fees as determined by the court.

d. An action to enforce any liability created under 5 U.S.C. § 552a may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where parties subject to this Agreement have materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under 5 U.S.C. § 552a, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action because of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

33.2 Criminal Penalties

a. Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000. See 5 U.S.C. § 552a(i)(1).

b. Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000. See 5 U.S.C. § 552a(i)(2).

c. Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000. See 5 U.S.C. § 552a(i)(3).

34 CHILD SUPPORT FPLS REQUIREMENTS

34.1 Contractor, when applicable and to the extent within Contractor's control, and the applicable State of Oklahoma agency must comply with the security requirements established by the Social Security Act, the Privacy Act of 1974, the Federal Information Security Management Act of 2002 (FISMA), 42 United States Code (USC) 654(26), 42 UCS 654a(d)(1)-(5), the U.S. Department of Health and Human Services (HHS), the U.S. Department of Health and Human Services Administration of Children and Families Office of Child Support Enforcement Security Agreement and the Automated Systems for Child Support Enforcement: A Guide for States Section H Security and Privacy. Contractor and applicable State of Oklahoma agency also agree to use Federal Parent Locator Service (FPLS) information and Child Support (CS) program information solely for the authorized purposes in accordance with the terms in this agreement. The information exchanged between state Child Support agencies and all other state program information must be used for authorized purposes and protected against unauthorized access to reduce fraudulent activities and protect the privacy rights of individuals against unauthorized disclosure of confidential information.

34.2 This is applicable to the personnel, facilities, documentation, data, electronic and physical records and other machine-readable information systems of the applicable State of Oklahoma agency and Contractor, including, but not limited to, state employees and contractors working with FPLS information and CS program information and state CS agency data centers, statewide centralized data centers, contractor data centers, state Health and Human Services' data centers, comprehensive tribal agencies, data centers serving comprehensive tribes, and any other individual or entity collecting, storing, transmitting or processing FPLS information and CS program information. This is applicable to all FPLS information, which consists of the National Directory of New Hires (NDNH), Debtor File, and the Federal Case Registry (FCR). The NDNH, Debtor File and FCR are components of an automated national information system.

34.3 This is also applicable to all CS program information, which includes the state CS program information, other state and tribal program information, and confidential information. Confidential information means any information relating to a specified individual or an individual who can be identified by reference to one or more factors specific to him or her, including but not limited to the individual's Social Security number, residential and mailing addresses, employment information, and financial information. Ref. 45 Code of Federal Regulations (CFR) 303.21(a).

35 FERPA REQUIREMENTS

35.1 If Contractor takes possession or control of Information covered by FERPA in performance of this Agreement, Contractor agrees to, when applicable and to the extent within Contractor's control comply with and assume responsibility for compliance by its employees with the Family Educational Rights and Privacy Act; (20 U.S.C. § 1232g; 34 CFR Part 99) ("FERPA") and the Oklahoma Student Data Accessibility, Transparency, and Accountability Act of 2013; (70 O.S. § 3-168), where personally identifiable student education data is exchanged.

36 CJIS REQUIREMENTS

36.1 INTRODUCTION - This section shall be applicable to the extent that Contractor takes possession or control of CJIS data. The use and maintenance of all items of software or equipment offered for purchase herein must be in compliance with the most current version of the U.S. Department of Justice, Federal Bureau of Investigation ("FBI"), Criminal Justice Information Services (CJIS) Division's CJIS Security Policy ("CJIS Security Policy" or "Security Policy" herein).

36.2 The Entity or Affiliate acquiring the data or system is hereby ultimately responsible for compliance with the CJIS Security Policy and will be subject to an audit by the State of Oklahoma CJIS Systems Officer ("CSO") and the FBI CJIS Division's Audit Staff.

36.3 CJIS SECURITY POLICY REQUIREMENTS GENERALLY - The CJIS Security Policy outlines a number of administrative, procedural, and technical controls agencies must have in place to protect Criminal Justice Information ("CJI"). Our experience is that agencies will generally have many of the administrative and procedural controls in place but will need to implement additional technical safeguards in order to be in complete compliance with the mandate. A Criminal Justice Agency ("CJA") and certain other governmental agencies procuring technology equipment and services that could be used in hosting or connecting or transmitting or receiving CJI data may need to use the check list herein to make sure that the software, equipment, location, security, and persons having the ability to access CJI will meet the CJIS requirements per the then current CJIS Security Policy. A completed Appendix H to said Security Policy will need to be signed by Vendor or a 3rd party if it has access to CJI, such as incident to the maintenance or support of the purchased hardware or software within which resides CJI. Per Appendix "A" to said Security Policy, "access to CJI is the physical or logical (electronic) ability, right or privilege to view, modify or make use of CJI."

36.4 DIRECTIVE CONCERNING ACCESS TO CRIMINAL JUSTICE INFORMATION AND TO HARDWARE OR SOFTWARE WHICH INTERACTS WITH CJI AND CERTIFICATION- The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities for criminal justice purposes, as well as the noncriminal justice communities for noncriminal justice purposes.

36.5 This Directive primarily concerns access to CJI and access to hardware and software in the use, retention, transmission, reception, and hosting of CJI for criminal justice purposes and not for noncriminal justice purposes. In that regard, this Directive is not only applicable to such data, but also to the hardware and software interacting with such data, their location(s), and persons having the ability to access such data. The CJIS data applicable to the Security Policy is the data described as such in said Policy plus all data transmitted over the Oklahoma Law Enforcement Telecommunications System ("OLETS") which is operated by DPS.

36.6 In order to have access to CJI or to the aforesaid hardware or software, the vendor must be familiar with the FBI CJIS Security Policy, including but not limited to the following portions of said Security Policy:

a. the Definitions and Acronyms in §3 & Appendices "A" & "B";

b. the general policies in §4;

c. the Policies in §5;

d. the appropriate forms in Appendices "D", "E", "F" & "H"; and

e. the Supplemental Guidance in Appendices "J".

36.7 This FBI Security Policy is located and may be downloaded at:

a. https://le.fbi.gov/file-repository/cjis_security_policy_v6-0_20241227.pdf/view

b. By executing the Contract to which this Directive is attached, the vendor hereby CERTIFIES that the foregoing directive has and will be followed, including but not limited to full compliance with the FBI CJIS Security Policy, as amended and as applicable.

37 NOTICES

37.1 In addition to notice requirements under the terms of the Contract otherwise, the following individuals shall also be provided the request, approval or notice, as applicable:

Chief Information Officer
3115 N. Lincoln Blvd
Oklahoma City, OK 73105

With a copy, which shall not constitute notice, to:
OMES Deputy General Counsel
2401 North Lincoln Blvd.
Oklahoma City, Oklahoma 73105

Request for Proposals for a New IFTA/ IRP System
Issued by the Oklahoma State Department of Corporation Commission (OCC)
Solicitation Number EV00000780
Bidder Name: Explore Information Services, LLC

7.7 Section Seven: Response to Specifications and Requirements,
EXHIBIT 4: MANDATORY SPECIFICATIONS, TECHNICAL RESPONSE

Offeror must provide complete and succinct responses to each item below. **Insert your responses into this worksheet directly into the yellow boxes** If your response does not fit into the boxes below a clearly labeled response (Example: 7.7.b etc). will be considered. Offeror should provide all information necessary to demonstrate Offeror's ability to meet the requirements of this RFP and the RFP's Scope of Work. Responses to the below questions in this Attachment are mandatory and will be evaluated. Failure to respond to any question may result in your proposal being deemed nonresponsive. Suppliers are to describe their specialized service and provide detailed information on their expertise and core competencies for each applicable specification of their response, to include the following information for Advertising specification. Broken out below for response ease. Bidder should respond to each Criteria per specification of application in the boxes below or site where this information can be found within their response. If the criterion does not apply to the specification, indicate Not Applicable (NA). Note: Suppliers may use the same project example for multiple specifications; however, work performed should be clearly identifiable as related to that single advertising specification for projects that have multiple categories.

This solicitation targets multiple bidders in order to meet the service requirements of the specification category expertise of the bid. Suppliers must demonstrate experience and core competencies providing services for customers that match the specification requirements of this solicitation. Overall, Suppliers must describe their specialized service and provide detailed information on their expertise and core competencies for each applicable specification category of their bid response. Please review the specification descriptions listed in Attachment A for specific information regarding the qualifications that would be needed by the Suppliers for those categories. The services listed in each specification are not exhaustive and Suppliers should bid under the specification and SOW that best represent the services being offered. Services that cannot easily be classified under other specification categories may be bid under the "Value Added" section of the solicitation.

	Meets Specification:	YES	NO	ADDITIONAL NOTES : (If using attachments provide Name of B
	Comply with all Plan requirements (IRP and IFTA Compacts), including:	YES		
I	International Registration Plan (IRP)	YES		The MCC system is fully aligned with the operational and audit requirements of the IRP and the Audit Procedures Manual (APM) maintained by IRP Inc. It supports all U.S. and Canadian jurisdictions affiliated with the IRP Plan and is designed to accommodate jurisdiction-specific rules, fee calculations, and audit protocols. The system includes automated IRP registration workflows, jurisdictional distance tracking, audit case management, and compliance reporting. Updates to IRP requirements are incorporated through our established change management and release processes to ensure ongoing compliance.
1	**Provide the following functionality (digitally):**			
1.)	Submit new applications i.) Meet Oklahoma state parameters around Continuous Registration	YES		Motor Carrier Connect (MCC) complies with Oklahoma's Continuous Registration requirements. The system includes built-in rules for all IRP jurisdictions to enforce continuous registration, ensuring uninterrupted compliance for new applications.
2.)	Submit renewal applications i.) Allow for 60-day grace period	YES		Motor Carrier Connect (MCC) supports a configurable 60-day grace period for renewal applications, in full compliance with Oklahoma's IRP/IFTA specifications.
3.)	Submit dispute forms	YES		Dispute forms can be uploaded into the MCC system and attached either to the specific application or at the account level. This functionality is supported with minor configuration adjustments. Refer to Section 07-01 Explore MCC Product Literature, Document Management.
4.)	Credential management:	YES		Refer to Section 07-01 Explore MCC Product Literature, Credentials Administration.
	i.) Tags: (a)Request replacement for lost, stolen, or damaged tags (b)Produce Tag Inventory (c)Assign Tag Inventory to Registrant	YES		Motor Carrier Connect (MCC) refers to "Tags" as Plates within the system. MCC supports the following credential management functions: **(a) Request Replacement for Lost, Stolen, or Damaged Plates** MCC allows registrants to request plate replacements through a streamlined workflow. Users can initiate a replacement request for lost, stolen, or damaged plates directly from their account dashboard. **(b) Produce Plate Inventory** MCC includes a comprehensive Inventory Management Subsystem that tracks plate inventory across multiple office locations. Inventory can be viewed, reported, and managed in real time, supporting both automatic and manual assignment methods. **(c) Assign Plate Inventory to Registrant** Authorized users can assign plate inventory to registrants either automatically (based on FIFO rules) or manually by selecting specific plate numbers. This ensures accurate tracking and assignment of credentials. Refer to Section 07-01 Explore MCC Product Literature, Credentials Administration, and Inventory Management.
	ii.) Cab Cards: (a)Reprint cab cards (b)Modify cab card information (c)45 Day Temporary Cab Cards (d)Ability for QR codes to be applied to cab cards that will take the officer to the system to verify the credentials when scanned	YES		Motor Carrier Connect (MCC) provides full support for cab card management, customized to meet Oklahoma's jurisdictional requirements. Key capabilities include: **(a) Reprint Cab Cards** Authorized users can reprint cab cards at any time through the MCC interface. Reprints are tracked and logged for audit purposes. **(b) Modify Cab Card Information** MCC allows modification of cab card data through supplement workflows. Changes are reflected in real-time and updated credentials can be issued immediately. **(c) 45-Day Temporary Cab Cards** MCC supports the issuance of temporary cab cards with configurable expiration periods. The 45-day validity is easily set based on Oklahoma's rules. **(d) QR Code Integration for Credential Verification** MCC cab cards can include QR codes that link directly to the system for credential verification. When scanned by enforcement officers, the QR code provides secure, real-time access to the credential record. Additionally, MCC enables Oklahoma to maintain jurisdiction-specific messaging on cab cards using the User Maintained Text utility. This allows the state to update cab card text independently, without requiring support from Explore. Refer to Section 07-01 Explore MCC Product Literature, Credentials Administration.
5.)	Upload vehicles in bulk	YES		Refer to Section 07-01 Explore MCC Product Literature, Vehicle Management.

	i.) Bulk Uploads: (a)Verification of load data limits (1)Other states with comparable fleet sizes (i)Large fleet data manipulation speed	YES		The MCC system demonstrates consistent and scalable performance when handling bulk vehicle uploads. Based on observed processing benchmarks: 100 units: Completed in approximately 15–17 seconds 1,000 units: Initiated processing within ~27 seconds; completed in ~2 minutes 5,000 units: Initiated after >10 minutes; completed in ~19 minutes 10,000 units: Initiated after >10 minutes; completed in ~32 minutes Once processing begins, throughput averages 10–12 records per second, supporting efficient handling of large fleet data. These metrics reflect MCC's capability to support jurisdictions with comparable fleet sizes and high-volume data operations.
6.)	Add or delete vehicles/fleets	YES		The MCC system supports adding and deleting vehicles through the IRP application and supplement process, with role-based security ensuring only authorized users can perform these actions. Users may initiate straight adds, straight deletes, or add-deletes (referred to as exchanges), which allow credit from the deleted vehicle to be applied to the added vehicle based on jurisdiction-specific credit rules published by IRP, Inc. Additionally, MCC supports fleet-to-fleet transfers within the same account, where a vehicle is deleted from one fleet and added to another. These transfers also follow the credit rules established by each jurisdiction and published by IRP, Inc. MCC ensures that all vehicle-related transactions, whether adds, deletes, exchanges, or transfers, adhere to the jurisdiction-specific credit rules published by IRP, Inc., supporting consistent and compliant fee calculations across all participating jurisdictions. Refer to Section 07-01 Explore MCC Product Literature, Vehicle Management.
	i.) Credits (Deletion) – Allowed by Compact but required by State Regulations (a) Allow deletion of vehicle in fleet with ability to apply credit to another truck added to same fleet for same registration period ii.) Change status of accounts, fleets, and vehicles within a fleet	YES		**i.) Credits (Deletion)** Motor Carrier Connect (MCC) supports credit management in accordance with the International Registration Plan (IRP) Agreement and Oklahoma state regulations. The system allows for the deletion of a vehicle within a fleet, and enables the application of the resulting credit to another vehicle added to the same fleet during the same registration period. **ii.) Change Status of Accounts, Fleets, and Vehicles** Motor Carrier Connect (MCC) provides authorized users with the ability to change the status of accounts, fleets, and vehicles using a role-based administrative interface. Status changes such as active, suspended, revoked, or canceled are managed through MCC's Restrictions Management subsystem, which is governed by security tasks to ensure proper access control. Each restriction is uniquely configured with a status code and associated deny points. These deny points can trigger downstream effects such as preventing fleet renewals, blocking the issuance of temporary or permanent credentials, etc. These restrictions are maintained by staff with the appropriate security authority and can be updated as needed to reflect evolving business rules. In addition to manual updates, MCC includes automated processes and system interfaces that can change the status of accounts based on predefined business logic. For example, account status may be automatically updated due to renewal activity, payment delinquencies, or other compliance-related conditions. All status changes and restriction applications are logged for audit purposes, ensuring transparency and accountability. This flexible framework allows Oklahoma to enforce its business rules while maintaining operational efficiency and regulatory compliance.
7.)	Modify vehicle weight	YES		Motor Carrier Connect (MCC) supports robust Weight Group Management for IRP fleets. Vehicle weights are organized into configurable weight groups at the fleet level, and each unit is assigned to a specific group. In addition to group weights, MCC maintains unladen weight directly on the vehicle record to support jurisdictional compliance and reporting. All weight modifications are performed through standard IRP application workflows, including renewals and supplements. During these transactions, users can create, update, or reassign weight groups, and move units between groups as needed. If a selected weight exceeds a jurisdiction's maximum allowed weight, MCC will trigger a validation error and prevent the record from being saved until the issue is resolved by the user. Maintaining weight groups and vehicle records is security task driven, ensuring that only users with appropriate authority can perform these updates. All changes are logged for audit purposes, supporting transparency and regulatory compliance. Refer to Section 07-01 Explore MCC Product Literature, Weight Group Management.
8.)	Update account information	YES		Motor Carrier Connect (MCC) allows authorized users to update account information through secure, role-based access. Users with the appropriate security tasks can modify key account details such as contact information, addresses, officer data, legal status, and preferred communication methods. All updates are tracked through audit logs to ensure transparency and accountability. MCC also supports account-level configuration options, including certified funds requirements, related account associations, and IFTA/IRP distribution preferences. These updates can be made directly by staff with the proper authority, without requiring intervention from Explore. Refer to Section 07-01 Explore MCC Product Literature, Account Management.
	i.) Allow company account to be managed by the company registrants regarding fleet information digitally	YES		Motor Carrier Connect (MCC) allows company registrants, including carriers and licensing agents (service providers), to manage account and fleet information digitally, based on the roles and permissions assigned by the state. All account and fleet maintenance functions are security task driven, meaning the state both defines and maintains what each user role is authorized to do through a Security Task Role Utility that operates live in production. MCC supports flexible configuration to enable external users to update specific account and fleet details. For example, address changes submitted by external users can be configured to enter a pending status, allowing state staff to review and approve or deny the update before it is finalized. This ensures both operational efficiency and oversight. This approach gives Oklahoma full control over user access while empowering registrants to manage their information securely and efficiently.
9.)	Print required documents	YES		Motor Carrier Connect (MCC) supports the identification and printing of documentation required to complete IRP transactions, such as proof of insurance, HVUT payment, and other jurisdiction-specific materials. The system automatically determines which documents are required based on the transaction activity within the IRP application. A "Required Materials" PDF report is generated for each application. This report can be viewed, printed, or emailed directly from the MCC system and provides a detailed breakdown of all required documents, organized by vehicle and document type. This ensures carriers and service providers have clear visibility into what must be submitted to receive permanent credentials. Refer to Section 07-01 Explore MCC Product Literature, Required Materials Management.

10.)	Ability to correct errors within the system and reverse processes as needed	YES		Motor Carrier Connect (MCC) provides authorized users with multiple tools to correct errors and reverse processes, ensuring flexibility and compliance with Oklahoma's business rules. **Retraction Supplements** Used when a vehicle was registered by mistake, this feature allows users to delete the vehicle and issue a full refund. Retraction supplements are also transmitted to the IRP Clearinghouse, ensuring that all member jurisdictions receive accurate and updated registration data. **Fee Correction Supplements** Enables users to adjust jurisdictional mileage for a fleet. MCC automatically recalculates all related supplements within the same registration year to ensure accurate fee assessment. These corrections are also transmitted to the IRP Clearinghouse to maintain consistency across jurisdictions. **Unfile Functionality** Allows users with appropriate security roles to unlock filed applications that have not yet been paid, enabling corrections before final processing. All correction and reversal actions are security task driven, meaning only users with the proper authority can perform these functions. Each action is logged for audit purposes, supporting transparency and regulatory compliance.
2	**Provide a public facing enforcement screen to allow officers to validate credentials**	YES		Motor Carrier Connect (MCC) is committed to supporting enforcement needs through a public-facing credential validation screen. While this feature is not currently available, it is part of our planned roadmap and will be developed to meet Oklahoma's enforcement requirements. Initially, enforcement officers will be able to validate credentials using QR codes printed on cab cards. When scanned, these QR codes will direct officers to a secure, public-facing screen that displays real-time credential information for the associated vehicle. This approach ensures quick, reliable access to credential data without requiring login credentials or full system access. As the feature evolves, MCC will work closely with Oklahoma to expand its functionality in alignment with jurisdictional needs and enforcement workflows.
3	**Maintain and update jurisdictional calculations for fleet vehicles**	YES		Motor Carrier Connect (MCC) offers comprehensive base and foreign jurisdiction fee processing capabilities based on the published IRP fee schedules. The MCC fee calculation engine determines fees according to the specific fee structures of each jurisdiction and allows for the creation of base jurisdiction-specific fees to accommodate unique requirements.
1.)	Maintain the fee calculator and update fees	YES		Explore's MCC IRP/IFTA system includes a robust and configurable Fee Calculator that supports all IRP and IFTA fee structures across jurisdictions. As part of our service agreement, Explore provides comprehensive support for fee maintenance and updates, ensuring accuracy and compliance with jurisdictional requirements. **Monitoring & Implementation:** Explore actively monitors all fee changes published by IRP jurisdictions via irponline.org. **Change Management Workflow:** - Fee changes are implemented in the MCC system upon publication. - Updates are moved to the QA environment for User Acceptance Testing (UAT). - Upon successful UAT, changes are deployed to Production. **Coordination & Communication:** - Explore coordinates all communication and code deployments with the base jurisdiction, ensuring transparency and alignment. - Notifications and documentation of fee changes are shared with stakeholders as part of our change control process. **Audit & Compliance:** - All fee updates are logged and auditable. - Historical fee data is retained for compliance and reporting purposes.
2.)	Enable performing annual fee tests	YES		Explore is actively engaged in the annual fee testing process to ensure accuracy and compliance with IRP/IFTA fee structures. Our approach is structured, collaborative, and fully aligned with jurisdictional expectations. **Test Execution in Lower Environment:** Explore initiates the annual fee test cycle by executing all required test scenarios in a lower environment. This allows for early identification of discrepancies and ensures system readiness before formal testing begins. **Documentation & Demonstration:** All test results are fully documented, including fee calculations, jurisdiction-specific logic, and waiver scenarios. Explore presents these findings to the customer in a collaborative review session, ensuring transparency and shared understanding. **Customer QA Testing Support:** After Explore's initial testing, the customer may choose to run additional tests in the QA environment. Explore provides guidance and support throughout this phase to ensure consistency and completeness. **Submission & Remediation:** The customer is responsible for submitting the final test results to the jurisdiction. If any issues arise, Explore works closely with the customer to remediate discrepancies, revalidate results, and ensure successful submission. **Jurisdictional Coordination:** Explore supports the customer in: - Running tests from the QA system - Completing required documentation - Submitting results to the jurisdiction for confirmation - Forwarding results to IRP, Inc. This structured and collaborative approach ensures that annual fee testing is thorough, accurate, and aligned with IRP, Inc. standards.
4	**Communication to/from registrants**			Explore's MCC IRP/IFTA system provides a secure, integrated communication framework that supports registrant engagement while complying with the confidentiality requirements of the Oklahoma Corporation Commission (OCC). The system includes the following capabilities:

1.)	Ability to upload documentation	YES		Registrants can securely upload required documentation directly into their account via the MCC portal. Uploaded files are automatically linked to the registrant's profile and associated transactions, ensuring traceability and ease of access for jurisdictional staff.
2.)	Communication tracking: Capture and maintain the communications within the registrant's file in the system	YES		All communications initiated by the registrant or jurisdiction staff are captured and stored within the registrant's file. This includes email exchanges, system-generated messages, notes, and attachments. The communication log is searchable and auditable to support operational and compliance needs.
3.)	Allow for email and SMS messaging to registrants that complies with confidentiality requirements of OCC	YES		The MCC system currently supports outbound email messaging to registrants. These communications are configurable by jurisdiction, logged within the registrant's file, and designed to comply with OCC confidentiality standards. While SMS messaging is not currently supported, Explore has plans to develop and implement SMS functionality in a future system release to enhance registrant communication options.
4.)	Allow for system notifications to registrants	YES		The MCC IRP/IFTA system delivers system-generated notifications to registrants through both real-time triggers and scheduled batch processes. **Real-time notifications** are automatically generated in response to specific system events, including: - User account requests such as password resets or profile updates - Online application submissions and status changes - Workflow re-assignments initiated by jurisdiction staff These notifications are sent immediately to ensure registrants and staff are informed of critical actions as they occur. **Scheduled batch notifications** are configured to run at defined intervals and support broader communication needs such as renewal reminders, compliance alerts, and informational updates. These are tailored to registrant groups based on criteria such as account status, expiration dates, or transaction history.
5	**Financial:** ***** Note: The internal IMS system will be the financial system of record, and an interface will be required.**			
1.)	Billing:			
	i.) Calculations function for users to generate estimated calculation without creating an invoice for planning purposes.	YES		Explore's MCC IRP/IFTA system provides users with the ability to perform fee calculations for planning purposes without generating an invoice or formally submitting an application. This is accomplished through the use of "in progress" supplements, which allow users to enter and modify application data freely. Users can calculate fees as many times as needed, enabling them to explore different scenarios and estimate costs before committing to a final submission. This functionality is especially valuable during the application process, as it allows users to evaluate the calculated results, identify any discrepancies, and make necessary corrections. Once the user is satisfied with the outcome, they can proceed to finalize the application and generate billing. This approach supports informed decision-making, improves accuracy, and enhances the overall user experience by providing flexibility and control throughout the process.
	ii.) Generate invoices based on the calculations when the user is ready to make a payment	YES		Explore's MCC IRP/IFTA system supports a structured and user-controlled invoicing process that begins with fee calculation and ends with the generation of an official billing invoice. Once fees have been calculated within an application in "In Progress" status, the user may proceed with filing the application. Filing the application transitions it to a "Filed" status, which locks the record to prevent further changes. This ensures the integrity of the submitted data and triggers the creation of an official invoice. The billing invoice includes all fees calculated during the application process. The display and grouping of these fees are configurable, allowing the jurisdiction to tailor how fees are presented to meet internal standards or registrant expectations. This flexibility supports clear communication of charges while maintaining consistency with jurisdictional financial practices.
	iii.) Ability to collect data around financial transaction information for reporting purposes, including batch information and batch IDs	YES		Explore's MCC IRP/IFTA system is equipped to collect and manage detailed financial transaction data to support jurisdictional reporting and reconciliation needs. The system captures all relevant financial activity, including payment details, transaction types, and associated metadata. For batch processing, the system assigns batch IDs to grouped transactions, allowing jurisdictions to track and report on financial activity by batch. This includes the ability to view batch totals, transaction counts, and processing timestamps. Batch information is stored alongside individual transaction records, enabling comprehensive reporting and audit traceability. Jurisdictions can generate reports filtered by batch ID, date range, payment method, or other financial attributes. These reports can be used for internal reconciliation, external financial system integration, and compliance documentation. The MCC system's reporting tools ensure that financial data is accessible, organized, and aligned with jurisdictional requirements.
	iv.) Ability to generate reports compliant with state requirements	YES		Explore's MCC IRP/IFTA system includes a wide range of standard financial reports, supports ad hoc reporting, and offers the ability to custom-build reports to meet Oklahoma's specific state requirements. This ensures flexibility in reporting while maintaining compliance with all mandated formats and standards.
	v.) Ability to report changes in prior period data in the current month of activity	YES		MCC is capable of generating reports that reflect changes to prior period data within the current month's activity.
	vi.) Generate reports which reflect historical data and trends	YES		MCC is capable of generating reports that reflect historical data and trends.
	vii.) Ability to incorporate clearinghouse reports	YES		We provide a variety of clearinghouse reports to support IRP processing and compliance. These include recaps and transmittals in PDF format.

	viii.) Interface with IMS and provide transactional data from invoices including all pass-thru revenue a.) This will be based around the OCC account ID that is generated in the IMS system. The selected system will need to use the OCC account ID as an identifier within the system. 1.) This would require name, address, and phone number be collected for sales of permits. b.) Timing of data transfers will need to be discussed.	YES		Explore's MCC IRP/IFTA system is designed to integrate securely and effectively with external financial systems, including Oklahoma's internal IMS system, which will serve as the financial system of record. **Interface with IMS** Explore will develop and maintain a secure interface that transmits transactional data from invoices, including all pass-through revenue, to the IMS system. This integration ensures that financial records are centralized and consistent with jurisdictional reporting requirements. **Use of OCC Account ID** The MCC system will incorporate the OCC account ID, generated by the IMS system, as a primary identifier for registrants. This ID will be used to associate financial transactions and registrant data across both systems, ensuring alignment and traceability. **Data Collection for Permit Sales** To support accurate financial reporting and integration, the MCC system will collect and transmit the following registrant details for permit sales: - Name - Address - Phone number These data elements will be linked to the OCC account ID and included in the transactional data sent to IMS. **Timing of Data Transfers** Explore will collaborate with Oklahoma's technical and financial teams to define the timing and frequency of data transfers. The system supports both real-time and scheduled batch processing, allowing flexibility based on operational and reporting needs. **Audit and Reconciliation** All financial transactions processed through MCC will be logged, auditable, and reconciled against IMS records. Explore will support reconciliation processes and provide detailed transaction histories as needed. **Collaboration and Testing** Explore will work closely with Oklahoma's team to define interface specifications, conduct integration testing, and validate data flows prior to production deployment.
	ix.) Provide information required to IMS to generate refunds for overpayments	YES		We have successfully implemented numerous financial interfaces that transmit detailed financial information, including refund data for overpayments. MCC supports providing the necessary information to IMS to initiate and process refunds, ensuring accurate reconciliation and alignment with jurisdictional financial workflows.
	x.) Ability to make corrections in the system to fix billing errors	YES		MCC allows authorized users to make corrections in the system to resolve billing errors through secure, task-driven workflows. One method includes adjusting fees either upward or downward, based on the nature of the correction and the user's assigned security permissions. In some instances, billing errors can be corrected by voiding the invoice. This is done by unfiling the transaction, making the necessary updates, and then refiling the application, which generates a new invoice with the corrected fee structure. All changes are tracked for audit purposes, ensuring transparency, accuracy, and compliance with financial controls.
	xi.) Interface with the payment processing system	YES		MCC supports integration with external payment processing systems to enable secure and efficient financial transactions. The system interfaces with third-party payment platforms to handle real-time authorization, settlement, and confirmation of payments. This allows registrants to pay using supported methods such as credit card, ACH, or other jurisdiction-approved options. Importantly, the contractual relationship with the third-party payment processor is between the vendor and the state, not Explore. Explore facilitates the technical integration and ensures that payment data is securely transmitted, properly logged, and reflected in the registrant's account and application status. The interface is configured and tested in collaboration with the jurisdiction to meet financial and security standards.
	xii.) Identify and maintain required payment types according to payment methods approved by agency rules a.) ACH – payment through QuickPay b.) Logic needs to be included that would provide a warning around restrictions around payment by check (would have to be certified funds)	YES		Explore's MCC IRP/IFTA system supports the identification and management of payment types in accordance with agency-approved methods and rules. The system allows jurisdictions to define and enforce accepted payment types, including ACH payments through QuickPay, as specified. Logic can be configured to provide warnings or restrictions for payment methods that require special handling. For example, if a registrant selects check as a payment method, the system can display a warning indicating that only certified funds are accepted, in compliance with agency rules.
	xiii.) Printed billing documents must contain a barcode supplied by IMS	YES		At present, the Motor Carrier Connect (MCC) system does not include barcodes on printed billing documents. However, Explore is fully committed to meeting this requirement and will work collaboratively with the Oklahoma Corporation Commission (OCC) to implement barcode functionality in alignment with IMS specifications. Explore will engage with OCC to gather the necessary technical requirements and ensure that barcodes provided by IMS are accurately incorporated into all relevant billing documents. This enhancement will be delivered through custom development and tested thoroughly to ensure compatibility, accuracy, and compliance with OCC's financial processing standards.
2.)	Provide necessary data to create Licensed Operator (LO) daily invoices to IMS	YES		Explore has successfully implemented financial interfaces for other jurisdictions that transmit detailed invoice data, including daily billing information. Explore will collaborate with the Oklahoma Corporation Commission (OCC) to define the specific data elements, formatting standards, and transmission protocols needed to support LO daily invoice generation. Leveraging our prior experience, we will configure and deploy a secure, reliable interface that ensures accurate and timely delivery of invoice data to IMS.
6	**Interface with IDR at IRP Inc.**	YES		Explore's Motor Carrier Connect (MCC) system successfully interfaces with IRP Inc.'s International Registration Plan Data Repository (IDR). This integration ensures timely and accurate transmission of registration data, including transmittals, recaps, and audit-related information, in compliance with IRP standards. The MCC system supports automated data exchange with IDR, including secure file transfers and validation protocols. Explore has implemented this interface in multiple jurisdictions and maintains ongoing compliance with IRP Inc. specifications through regular updates and coordination with IRP Inc. Refer to Section 07-01 Explore MCC Product Literature, IRP Clearinghouse Interface.

7	**Reports (30 reports)**	YES		**Reporting** MCC provides an extensive suite of reporting tools, including standard canned reports, scheduled reports, and powerful ad-hoc reporting options. These reports support operational, compliance, and analytical needs across IRP, IFTA, Audits, Security, Inventory, Account Management, and more! **Canned Reports** Explore offers a wide variety of pre-built reports that cover core business functions. These reports are available in multiple formats including HTML, PDF, Microsoft® Excel®, and CSV. Each report includes a built-in dynamic filtering text box within the data grid. As users type into the filter, the system automatically narrows the displayed records to those containing matching text in any column, allowing for quick, intuitive refinement without needing to export or re-run the report. **Ad-Hoc Reporting** The ad-hoc reporting feature is highly flexible and virtually limitless in scope. Explore can create and deploy custom, nonstandard reports directly into production without code moves, making them immediately available for use. These reports can be re-run at any time and are downloadable in CSV format, providing ongoing access to critical data without requiring technical expertise or system downtime. **Self-Service Reporting** MCC includes Easy Query, a true self-service ad-hoc reporting tool that empowers users to create, save, share, search, and export customized reports independently. Users can build reports using intuitive filters and field selections, with output available in multiple formats including CSV for easy data manipulation. All reporting features are governed by role-based security controls to ensure appropriate access and data protection. MCC's reporting framework supports transparency, operational oversight, and informed decision-making across all levels of jurisdictional operations.
8	**Documentation:**			
1.)	Laserfiche will be the document management system of record for imaging and documentation storage	YES		The Motor Carrier Connect (MCC) system supports document upload functionality as part of its core capabilities. To meet Oklahoma's requirement that Laserfiche will be the document management system of record, MCC will be designed to interface directly with Laserfiche for seamless transmission of uploaded documents. We acknowledge that Laserfiche will serve as the authoritative repository for imaging and documentation storage. Accordingly, MCC will implement a robust and secure integration that accommodates Laserfiche's specifications, ensuring all relevant documents are transferred appropriately and reliably. This interface will be developed in alignment with Oklahoma's technical and operational standards for document management.
9	**Provide mobile version for users (either mobile friendly website or app)**	YES		The Motor Carrier Connect (MCC) IRP/IFTA system is designed with a responsive, mobile-friendly web interface that ensures full functionality across desktop, tablet, and smartphone devices. Users can access the system securely via standard mobile browsers without requiring a separate mobile application. The interface adapts dynamically to various screen sizes, maintaining usability and performance for tasks such as account management, application submission, document uploads, and payment processing without requiring a separate mobile application.
II	**IFTA - International Fuel Tax Agreement**	YES		Our Motor Carrier Connect (MCC) system is fully compliant with the operational requirements outlined in the IFTA Procedure Manual and Audit Manual. The system is designed to support all jurisdictions participating in the IFTA agreement, including the 48 contiguous U.S. states and the 10 Canadian provinces. Compliance is maintained through regular updates aligned with IFTA regulatory changes, and our audit functionality ensures adherence to IFTA standards. The system also supports electronic filing, jurisdictional reporting, and audit tracking as required by IFTA.
1	**Oklahoma is an Option 2 state for IFTA Quarterly returns**	YES		Motor Carrier Connect (MCC) complies with all IFTA Transmittal requirements, including support for both Option 1 and Option 2 reporting formats. As Oklahoma is an Option 2 state, MCC will be configured to transmit quarterly return data in accordance with Option 2 specifications. This ensures seamless integration with Oklahoma's reporting processes and compliance with jurisdictional standards.
2	**Provide online access for Licensees to:**			
1.)	Submit new applications i. Meet Oklahoma state parameters	YES		The Motor Carrier Connect (MCC) IRP/IFTA system provides licensees with secure online access to initiate new account applications. Applicants can enter and manage essential information including contacts, officers, physical and mailing addresses, IFTA license details, user accounts, and the number of decals required. The system also supports uploading required documents based on Oklahoma's configurable rules. State administrators have full access to review, update, approve, or deny applications within the system. Automated email notifications are sent to applicants at each status change, ensuring transparency and timely communication throughout the application process. MCC's configuration ensures full compliance with Oklahoma's state parameters for new account setup.
2.)	Submit renewal applications	YES		The Motor Carrier Connect (MCC) IRP/IFTA system allows licensees to submit renewal applications directly through the web application. The renewal process is guided by a step-by-step workflow that clearly outlines each required action, ensuring a user-friendly experience. All renewal activities are security task-driven, and the system performs real-time validation checks during both data entry and submission. If all validation rules are satisfied, the renewal is automatically completed without requiring intervention from Oklahoma staff. This efficient process ensures compliance with Oklahoma's renewal requirements while minimizing administrative effort.

3.)	Credential management: i. Decals: (a) Request replacement for damaged decals (b) Produce Decal Inventory (c) Request additional decals 1.) Up to 25% above fleet size on renewals and decal requests	YES		The Motor Carrier Connect (MCC) IRP/IFTA system provides secure, role-based credential management through the web application. Licensees can: - Request replacement decals for damaged items - Request additional decals, including up to 25% above fleet size during renewals and decal requests The 25% validation rule is configurable and will be set according to Oklahoma's specific requirements. MCC includes robust decal inventory reporting capabilities. Licensees can generate reports by account, showing all decals issued for a specific account by registration year. Additionally, the inventory management module provides detailed reports for administrators, including views of decals that are available, assigned, issued, or pending. These reports support operational oversight and ensure accurate tracking of decal distribution and availability. All decal-related actions are controlled through security permissions and are subject to license status. Only accounts in good standing, without restrictions that would prevent ordering, are permitted to request additional decals. MCC enforces these conditions through configurable validation rules and automated checks to ensure compliance and accuracy.
4.)	Submit quarterly returns i. Include ability for warnings and stop flags for bad data (a) More discussion would be required to outline what these are ii. Include the ability to upload quarterly return data in the form of Excel files to the system iii. Ability to submit amended returnsiv. Capability to print paper returns v. Ability to enter information from paper returns into the system vi. Ability to update interest information as required	YES		The Motor Carrier Connect (MCC) IRP/IFTA system provides licensees with secure access through the web application to submit quarterly returns. The system supports the following capabilities: **Warnings and stop flags for bad data:** MCC includes configurable validation logic that incorporates all IFTA Clearinghouse data quality checks. In addition, the MCC system includes minimum and maximum MPG thresholds, contiguous jurisdiction checks. The MCC system also validate when taxable and total distance are the same. In such cases, carriers are allowed to save the return but must enter a comment explaining the reason. Further discussion with Oklahoma will be required to define additional warning and stop flag criteria. **Excel file upload:** Licensees can upload quarterly return data using CSV and XML file formats. The system parses and validates the uploaded data before submission. If validation errors are encountered, the system can "shelf" the return, allowing the user to log in and correct the data, or enabling Oklahoma staff to override the error based on approved scenarios. Email notifications are automatically sent to inform users of the upload status. **Amended returns:** Users can submit amended returns through the same workflow. The system requires users to enter a comment or reason for amending the return, and all changes are tracked through audit logs and validation checks. **Print paper returns:** The system generates a PDF version of the quarterly return, which can be printed and manually completed by the user. This PDF can be produced via a batch job for mailing by staff, or generated on demand by either the carrier or Oklahoma staff within the system. **Enter paper return data:** Oklahoma staff can manually enter data from paper returns into the system, ensuring all returns are captured regardless of submission method. **Update interest information:** The system automatically calculates late interest based on the postmark date of the return. Authorized users have the ability to backdate the postmark date when necessary. All actions are governed by security roles and license status to ensure only authorized users can perform these tasks.
5.)	Update account information i. Allow company licensee to digitally manage account informat	YES		The Motor Carrier Connect (MCC) IRP/IFTA system allows company licensees to digitally manage their account information through the web application. Authorized users can update key account details including contacts, officers, physical and mailing addresses, and user access settings. All updates are controlled through security roles to ensure only permitted users can make changes. Changes are tracked through audit logs, and validation rules are applied to ensure data integrity. The system supports real-time updates and provides confirmation of successful changes. This functionality ensures licensees can maintain accurate and up-to-date account records in compliance with Oklahoma's requirements.
6.)	Print licenses	YES		The Motor Carrier Connect (MCC) IRP/IFTA system allows authorized users to generate and print IRP and IFTA licenses directly through the web application. Licenses are produced in PDF format and can be printed on demand by either the licensee or Oklahoma staff. The system supports batch printing for bulk processing and mailing, as well as individual license generation for immediate access. All license printing functions are governed by security roles to ensure only authorized users can perform these actions. License status is validated prior to printing to ensure only active and approved licenses are issued.
7.)	Ability to correct errors within the system and reverse processes as needed	YES		The Motor Carrier Connect (MCC) IRP/IFTA system provides robust functionality for correcting errors and reversing processes, all governed by security roles and license status. Key capabilities include: **Licenses:** Users can unfile or modify a license record if corrections are needed. This includes updating license details prior to finalization or correcting data entry errors. All changes are tracked and subject to validation rules. **Decals:** Decals can be unfiled to allow corrections. If a decal is lost or stolen, it can be cancelled with a required reason entered by the user. In cases where a decal was cancelled by mistake, the system allows reinstatement. All decal actions are logged and controlled through security permissions. **Returns:** Users can submit amended returns when corrections are needed. Additionally, the system allows reversal of previously submitted returns or amendments. All amended and reversed returns are transmitted to the IFTA Clearinghouse, ensuring compliance with reporting standards and maintaining data integrity.
3	**Provide a public facing enforcement screen to allow officers to validate credentials**	YES		Motor Carrier Connect (MCC) is committed to supporting enforcement needs through a public-facing credential validation screen. While this feature is not currently available, it is part of our planned roadmap and will be developed to meet Oklahoma's enforcement requirements. Initially, enforcement officers will be able to validate credentials using QR codes printed on cab cards. When scanned, these QR codes will direct officers to a secure, public-facing screen that displays real-time credential information for the associated vehicle. This approach ensures quick, reliable access to credential data without requiring login credentials or full system access. As the feature evolves, MCC will work closely with Oklahoma to expand its functionality in alignment with jurisdictional needs and enforcement workflows.

4	**Interface with IFTA Inc. to maintain and update tax rate matrix and fuel types**	YES		
1.)	The tax matrix would need to be downloaded for use in quarterly tax return calculations	YES		The Motor Carrier Connect (MCC) IRP/IFTA system interfaces with IFTA Inc. to retrieve and maintain the latest tax rate matrix and fuel types. The tax matrix is downloaded and stored within the system for use in quarterly return calculations. Updates are applied automatically based on IFTA Inc. schedules and formats. As part of our support agreement, our support team actively monitors and manages this process to ensure timely and accurate updates.
2.)	Potential to calculate distance tax in addition to a fuel tax on the same return	YES		MCC supports the configuration and calculation of both fuel tax and distance-based tax within the same quarterly return based on each jurisdictions' rules per fuel type.
3.)	Allow ability to process split tax rates	YES		The Motor Carrier Connect (MCC) IRP/IFTA system includes the ability to process split tax rates as defined by IFTA Inc. These rates are applied based on jurisdiction and effective date, ensuring accurate tax calculations across varying rate periods within a single quarter. In addition, the system displays the split rates and their effective dates on the return tax form, within the data entry screen, and on the return summary. This makes it clear to the taxpayer that data must be entered according to the applicable rate periods.
5	**Communication to/from registrants**			Refer to Section 07-01 Explore MCC Product Literature, Communications / Correspondence Management.
1.)	Ability to upload documentation	YES		The Motor Carrier Connect (MCC) IRP/IFTA system allows registrants to securely upload documentation through the web application. Document upload functionality is available during workflows such as new account setup, renewals, and user account management. The system supports multiple file formats and enforces validation rules to ensure required documents are submitted based on Oklahoma's configuration. Uploaded documents are stored securely and are immediately accessible to authorized state staff for review. All upload actions are tracked through audit logs, and email notifications can be triggered based on submission status or document review outcomes.
2.)	Communication tracking: Capture and maintain the communications within the registrant's file in the system	YES		The Motor Carrier Connect (MCC) IRP/IFTA system includes built-in communication tracking that captures and stores all relevant communications within the registrant's account file. This includes system-generated messages, email notifications, and staff-entered notes or correspondence. Communications are timestamped and associated with specific actions or workflows, such as application submissions, approvals, or document reviews. Authorized users can view the full communication history for each registrant, ensuring transparency and continuity in case management. All entries are governed by security roles and retained according to configurable retention policies.
3.)	Allow for email and SMS messaging to registrants that complies with confidentiality requirements of OCC	YES		The MCC system currently supports outbound email messaging to registrants. These communications are configurable by jurisdiction, logged within the registrant's file, and designed to comply with OCC confidentiality standards. While SMS messaging is not currently supported, Explore has plans to develop and implement SMS functionality in a future system release to enhance registrant communication options.
4.)	Allow for system notifications to registrants	YES		The MCC IRP/IFTA system delivers system-generated notifications to registrants through both real-time triggers and scheduled batch processes. **Real-time notifications** are automatically generated in response to specific system events, including: - User account requests such as password resets or profile updates - Online application submissions and status changes - Workflow re-assignments initiated by jurisdiction staff These notifications are sent immediately to ensure registrants and staff are informed of critical actions as they occur. **Scheduled batch notifications** are configured to run at defined intervals and support broader communication needs such as renewal reminders, compliance alerts, and informational updates. These are tailored to registrant groups based on criteria such as account status, expiration dates, or transaction history.
6	**Financial:** ***** Note: The internal IMS system will be the financial system of record, and an interface will be required.**			
1.)	Billing:			

	i.) Generate invoices based on the quarterly return (a.) This would include refund from fuel usage reconciliation (b.) Update the interest calculations based on the current date/month (c.) Identify non-filers (as a report) and include penalties.	YES		The Motor Carrier Connect (MCC) IRP/IFTA system automatically generates invoices based on the data submitted in quarterly returns. The billing process includes: **Refunds from fuel usage reconciliation:** When a return results in a credit, and the account is in good standing with no restrictions preventing refund requests, the taxpayer may request the refund immediately at the time of filing. This is allowed if the credit amount falls within the Oklahoma Corporation Commission's (OCC) configurable minimum and maximum refund thresholds. The refund request process is security task-driven and subject to validation. **Interest calculations:** Late filing interest is initially calculated at the time the return is filed and the invoice is generated. After filing, MCC continues to evaluate unpaid invoices monthly and automatically applies additional interest based on the current date. This ensures accurate and up-to-date interest accrual for outstanding balances. **Identification of non-filers:** The MCC IRP/IFTA system includes a robust, automated multi-cycle process to manage non-filers: **- Automated Evaluation Cycles:** MCC continuously monitors accounts for missing returns. When a return is not filed, the system initiates a configurable multi-cycle notification process. **- Notice Generation:** For each cycle, MCC automatically generates a non-filing notice and applies a restriction to the account. These notices escalate in severity with each cycle. **- Penalty Enforcement:** After a configurable number of notices (commonly the third), MCC can automatically generate a reinstatement penalty. If the taxpayer eventually files the late return, MCC calculates the late filing penalty automatically. This penalty is typically the greater of $50 or 10% of the tax due, based on Oklahoma's configuration. **- Reporting & Follow-Up:** MCC provides staff with reporting tools to identify non-filers and track penalty assessments. These tools support enforcement and compliance efforts. **- Security & Audit:** All billing actions, including notices and penalties, are governed by security roles and tracked via audit logs to ensure transparency and accuracy.
	ii.) Generate invoices for reinstatement and decals when the user is ready to make payment	YES		The MCC IRP/IFTA system automatically generates invoices for reinstatement and decals based on user actions and system-driven delinquency processes: **Reinstatement Invoice Generation:** Reinstatement invoices are triggered by MCC's automated late filing or late payment delinquency notification processes. When an account reaches a configured threshold of non-compliance (e.g., after multiple missed filings or unpaid balances), the system generates a reinstatement invoice as part of the enforcement workflow. **Decal Invoice Generation:** When a user initiates a request for decals and the account is eligible, MCC generates the decal invoice immediately, applying fees based on Oklahoma Corporation Commission (OCC) configurations. **Configurable Fee Logic:** Both reinstatement and decal fees are applied according to OCC-defined rules, ensuring accurate and compliant billing. **Security and Audit Controls:** All invoice generation actions are governed by user security roles and tracked in audit logs for transparency and accountability. **Integrated Payment Readiness:** Once generated, invoices are available for immediate payment through MCC's integrated payment module, supporting secure and efficient transactions.
	iii.) Ability to collect data around financial transaction information for reporting purposes, including batch information and batch IDs	YES		Explore's MCC IRP/IFTA system is equipped to collect and manage detailed financial transaction data to support jurisdictional reporting and reconciliation needs. The system captures all relevant financial activity, including payment details, transaction types, and associated metadata. For batch processing, the system assigns batch IDs to grouped transactions, allowing jurisdictions to track and report on financial activity by batch. This includes the ability to view batch totals, transaction counts, and processing timestamps. Batch information is stored alongside individual transaction records, enabling comprehensive reporting and audit traceability. Jurisdictions can generate reports filtered by batch ID, date range, payment method, or other financial attributes. These reports can be used for internal reconciliation, external financial system integration, and compliance documentation. The MCC system's reporting tools ensure that financial data is accessible, organized, and aligned with jurisdictional requirements.
	iv.) Ability to generate reports compliant with state requirements	YES		Explore's MCC IRP/IFTA system includes a wide range of standard financial reports, supports ad hoc reporting, and offers the ability to custom-build reports to meet Oklahoma's specific state requirements. This ensures flexibility in reporting while maintaining compliance with all mandated formats and standards.
	v.) Ability to report changes in prior period data in the current month of activity	YES		MCC is capable of generating reports that reflect changes to prior period data within the current month's activity.
	vi.) Generate reports which reflect historical data and trends	YES		MCC is capable of generating reports that reflect historical data and trends.
	vii.) Ability to incorporate clearinghouse reports	YES		The MCC IRP/IFTA system provides robust support for incorporating and managing clearinghouse reports to ensure accurate IFTA processing and jurisdictional compliance: **Clearinghouse Report Support:** MCC offers a variety of clearinghouse reports, including transmittals in PDF format, to support jurisdictional data exchange and compliance tracking. **Return-Level Visibility:** At the individual return level, users can view the exact data that was transmitted to the clearinghouse. This includes jurisdictional tax details, mileage, and fuel usage. It also includes financial information remaining to be sent for jurisdictions using Option 1 for transmittals.

	viii.) Interface with IMS and provide transactional data from invoices including all pass-thru revenue a.) This will be based around the OCC account ID that is generated in the IMS system. The selected system will need to use the OCC account ID as an identifier within the system. 1.) This would require name, address, and phone number be collected for sales of permits. b.) Timing of data transfers will need to be discussed.	YES		Explore's MCC IRP/IFTA system is designed to integrate securely and effectively with external financial systems, including Oklahoma's internal IMS system, which will serve as the financial system of record. **Interface with IMS** Explore will develop and maintain a secure interface that transmits transactional data from invoices, including all pass-through revenue, to the IMS system. This integration ensures that financial records are centralized and consistent with jurisdictional reporting requirements. **Use of OCC Account ID** The MCC system will incorporate the OCC account ID, generated by the IMS system, as a primary identifier for registrants. This ID will be used to associate financial transactions and registrant data across both systems, ensuring alignment and traceability. **Data Collection for Permit Sales** To support accurate financial reporting and integration, the MCC system will collect and transmit the following registrant details for permit sales: - Name - Address - Phone number These data elements will be linked to the OCC account ID and included in the transactional data sent to IMS. **Timing of Data Transfers** Explore will collaborate with Oklahoma's technical and financial teams to define the timing and frequency of data transfers. The system supports both real-time and scheduled batch processing, allowing flexibility based on operational and reporting needs. **Audit and Reconciliation** All financial transactions processed through MCC will be logged, auditable, and reconciled against IMS records. Explore will support reconciliation processes and provide detailed transaction histories as needed. **Collaboration and Testing** Explore will work closely with Oklahoma's team to define interface specifications, conduct integration testing, and validate data flows prior to production deployment.
	ix.) Provide information required to IMS to generate refunds for overpayments	YES		We have successfully implemented numerous financial interfaces that transmit detailed financial information, including refund data for overpayments. MCC supports providing the necessary information to IMS to initiate and process refunds, ensuring accurate reconciliation and alignment with jurisdictional financial workflows.
	x.) Ability to make corrections in the system to fix billing errors	YES		MCC allows authorized users to make corrections in the system to resolve billing errors through secure, task-driven workflows. One method includes adjusting fees either upward or downward, based on the nature of the correction and the user's assigned security permissions. In some instances, billing errors can be corrected by voiding the invoice. This is done by unfiling the transaction, making the necessary updates, and then refiling the application, which generates a new invoice with the corrected fee structure. All changes are tracked for audit purposes, ensuring transparency, accuracy, and compliance with financial controls.
	xi.) Interface with the payment processing system	YES		MCC supports integration with external payment processing systems to enable secure and efficient financial transactions. The system interfaces with third-party payment platforms to handle real-time authorization, settlement, and confirmation of payments. This allows registrants to pay using supported methods such as credit card, ACH, or other jurisdiction-approved options. Importantly, the contractual relationship with the third-party payment processor is between the vendor and the state, not Explore. Explore facilitates the technical integration and ensures that payment data is securely transmitted, properly logged, and reflected in the registrant's account and application status. The interface is configured and tested in collaboration with the jurisdiction to meet financial and security standards.
	xii.) Identify and maintain required payment types according to payment methods approved by agency rules a.) ACH – payment through QuickPay	YES		Explore's MCC IRP/IFTA system supports the identification and management of payment types in accordance with agency-approved methods and rules. The system allows jurisdictions to define and enforce accepted payment types, including ACH payments through QuickPay, as specified. Logic can be configured to provide warnings or restrictions for payment methods that require special handling. For example, if a registrant selects check as a payment method, the system can display a warning indicating that only certified funds are accepted, in compliance with agency rules.
	xiii.) Printed billing documents must contain a barcode supplied by IMS	YES		At present, the Motor Carrier Connect (MCC) system does not include barcodes on printed billing documents. However, Explore is fully committed to meeting this requirement and will work collaboratively with the Oklahoma Corporation Commission (OCC) to implement barcode functionality in alignment with IMS specifications. Explore will engage with OCC to gather the necessary technical requirements and ensure that barcodes provided by IMS are accurately incorporated into all relevant billing documents. This enhancement will be delivered through custom development and tested thoroughly to ensure compatibility, accuracy, and compliance with OCC's financial processing standards.
7	**Interface with IFTA Clearinghouse**	YES		The MCC IRP/IFTA system interfaces seamlessly with the IFTA Clearinghouse and fully supports both Option 1 and Option 2 jurisdictions. Transmittals are submitted monthly, and the specific day of the month as well as whether the submission includes only the previous month or all data up to the current run is configurable. MCC complies with all IFTA Clearinghouse data file requirements, and our support team actively manages the transmittal process to ensure successful and accurate data uploads. Refer to Section 07-01 Explore MCC Product Literature, IFTA Clearinghouse Interface.
8	**Interface with IFTA Demographics (Daily)**	YES		The MCC IRP/IFTA system interfaces with the IFTA Demographics service on a daily basis and is fully compliant with IFTA's file format and data requirements. As part of this integration, MCC transmits carrier demographic data covering a configurable historical period, typically set to five years. This ensures that jurisdictions have access to accurate and comprehensive carrier information for audit, enforcement, and compliance purposes. Refer to Section 07-01 Explore MCC Product Literature, IFTA Clearinghouse Interface.

9	**Reports – canned, custom, and ad hoc reporting capability**	YES		**Reporting** MCC provides an extensive suite of reporting tools, including standard canned reports, scheduled reports, and powerful ad-hoc reporting options. These reports support operational, compliance, and analytical needs across IRP, IFTA, Audits, Security, Inventory, Account Management, and more! **Canned Reports** Explore offers a wide variety of pre-built reports that cover core business functions. These reports are available in multiple formats including HTML, PDF, Microsoft® Excel®, and CSV. Each report includes a built-in dynamic filtering text box within the data grid. As users type into the filter, the system automatically narrows the displayed records to those containing matching text in any column, allowing for quick, intuitive refinement without needing to export or re-run the report. **Ad-Hoc Reporting** The ad-hoc reporting feature is highly flexible and virtually limitless in scope. Explore can create and deploy custom, nonstandard reports directly into production without code moves, making them immediately available for use. These reports can be re-run at any time and are downloadable in CSV format, providing ongoing access to critical data without requiring technical expertise or system downtime. **Self-Service Reporting** MCC includes Easy Query, a true self-service ad-hoc reporting tool that empowers users to create, save, share, search, and export customized reports independently. Users can build reports using intuitive filters and field selections, with output available in multiple formats including CSV for easy data manipulation. All reporting features are governed by role-based security controls to ensure appropriate access and data protection. MCC's reporting framework supports transparency, operational oversight, and informed decision-making across all levels of jurisdictional operations.
1.)	Ability to combine multiple sources/types of data in reporting	YES		MCC supports combining multiple sources and types of data within its reporting tools. Users can generate reports that pull from various modules such as IRP, IFTA, Audit, Inventory, and Account Management, allowing for consolidated views across the system. Both canned and ad-hoc reports can include data from multiple tables, and Easy Query enables users to build custom reports that span functional areas, with export options including CSV, Excel, and PDF.
10	**Provide mobile version for users (either mobile friendly website or app)**	YES		The Motor Carrier Connect (MCC) IRP/IFTA system is designed with a responsive, mobile-friendly web interface that ensures full functionality across desktop, tablet, and smartphone devices. Users can access the system securely via standard mobile browsers without requiring a separate mobile application. The interface adapts dynamically to various screen sizes, maintaining usability and performance for tasks such as account management, application submission, document uploads, and payment processing without requiring a separate mobile application.
III	**IFTA/IRP Audit**			
1	**Oklahoma is an Option 1 state for IFTA/IRP Audits**	YES		The MCC IRP/IFTA system complies fully with IFTA Clearinghouse requirements, including support for both Option 1 and Option 2 jurisdictions. While Option 1 and Option 2 designations apply specifically to IFTA Clearinghouse transmittals, MCC is configured to meet the data formatting and transmission standards for each. The system ensures accurate and timely submission of required data, and our support team actively monitors and manages the process to guarantee successful uploads in accordance with IFTA specifications.
2	**Ability to post the audit to the Clearinghouse but not send line-item detail until the Audit bill is paid.**	YES		Posting audit summary reports/records to the Clearinghouse is currently a manual process and is not dependent on payment status. For IRP audits, MCC transmits audit financial data only after the audit bill has been paid in full. For IFTA audits, for Option 1 protocols, MCC transmits the foreign jurisdictions' credit records to IFTA with the first transmittal after filing, and the remaining financial data incrementally as payments are received. This approach ensures compliance with IFTA Clearinghouse requirements while aligning with Oklahoma's operational practices.
3	**Provide online access for Auditees to:**	YES		
1.)	Submit requested audit information	YES		The MCC IRP/IFTA system includes a robust Audit Correspondence module that streamlines communication between the state and auditees during the audit process. States can create and manage correspondence templates commonly used throughout audits. These templates support user-defined fields that dynamically pull data directly from the audit case, such as account number, registrant name, and audit-specific details. This ensures consistency and accuracy in communications. All audit correspondence is tracked within the system, from generation to user access, providing full visibility into delivery and engagement. Correspondence can be printed and mailed or emailed directly to the registrant/taxpayer, offering flexibility in how information is shared and ensuring timely submission of requested audit materials. Refer to Section 07-01 Explore MCC Product Literature, Document Management.
2.)	View status of audit	YES		The MCC IRP/IFTA system provides auditees with basic visibility into the status of their audit through the online portal. While detailed audit tracking is reserved for internal users, auditees can view whether an audit is in progress via workflow indicators or system flags. Additionally, they have access to any audit correspondence sent through the system, which helps them stay informed of requests and updates. This limited status view ensures auditees are aware of active audits and can respond appropriately, while maintaining the integrity of the audit process. Refer to Section 07-01 Explore MCC Product Literature, Audit Management
3.)	Update account information	YES		The MCC IRP/IFTA system allows auditees to update select account information through the online portal. Depending on jurisdictional configuration and security roles, auditees may be able to submit changes to contact details, mailing addresses, and other profile-related data. These updates are subject to validation and approval workflows as defined by the state. This functionality helps ensure that account records remain current and accurate throughout the audit process.
4.)	Print required documents	YES		While printing required documents is most commonly used during renewals, supplements, and similar processes, the MCC IRP/IFTA system also supports this functionality during audits when needed. If the state requires specific documentation to be printed as part of the audit process, MCC provides auditees with the ability to do so. Auditees can print a report indicating which documents are required or reprint documents they previously uploaded. This ensures flexibility and supports compliance with jurisdictional audit procedures.
4	**Maintain and update jurisdictional calculations for fleet vehicles**	YES		The MCC IRP/IFTA system ensures accurate jurisdictional calculations for fleet vehicles through a centralized configuration managed entirely by Explore. Explore maintains 100% of the jurisdictional rules, rates, and calculation logic used within the system. This includes updates to mileage allocations, fuel tax rates, and jurisdiction-specific requirements. By managing these configurations centrally, Explore ensures consistency, compliance, and accuracy across all fleet-related filings and transactions.

5	**Interface with IFTA Inc. to maintain and update tax rate matrix and fuel types**	YES		
1.)	Allow ability to process split tax rates.	YES		The Motor Carrier Connect (MCC) IRP/IFTA system includes the ability to process split tax rates as defined by IFTA Inc. These rates are applied based on jurisdiction and effective date, ensuring accurate tax calculations across varying rate periods within a single quarter. In addition, the system displays the split rates and their effective dates on the return tax form, within the data entry screen, and on the return summary. This makes it clear to the taxpayer that data must be entered according to the applicable rate periods.
2.)	The tax matrix would need to be downloaded for use in quarterly tax return calculations	YES		The Motor Carrier Connect (MCC) IRP/IFTA system interfaces with IFTA Inc. to retrieve and maintain the latest tax rate matrix and fuel types. The tax matrix is downloaded and stored within the system for use in quarterly return calculations. Updates are applied automatically based on IFTA Inc. schedules and formats. As part of our support agreement, our support team actively monitors and manages this process to ensure timely and accurate updates.
3.)	Potential to calculate distance tax in addition to a fuel tax on the same return	YES		MCC supports the configuration and calculation of both fuel tax and distance-based tax within the same quarterly return based on each jurisdictions' rules per fuel type.
6	**Update the interest calculation based on the current date/month**	YES		To update the audit interest calculation based on the current date or month, the MCC system uses a monthly proration method that evaluates each audit return period up to the "Interest Through Date" entered by the auditor during the "Save and Calculate" process. The system calculates interest by year, quarter, fuel type, and jurisdiction, ensuring that the interest reflects the most current applicable rates. If there has been a change in the interest rate, MCC applies the correct rate for each month based on its effective date. For example, if an audit spans several months and the rate changed midway, MCC will apply the older rate for the earlier months and the new rate for the remaining months. Credits generated from previous returns are not applied during the audit interest calculation but can be used to reduce the audit invoice after filing. Additionally, MCC ensures that interest is only calculated for periods where the audit invoice due date or the interest through date is past the current date, and the audit is not part of a payment plan. This dynamic approach ensures that interest is accurately calculated and updated in alignment with the current month and jurisdiction-specific rules.
7	**Apply state-determined penalties per calculation**	YES		For both IFTA and IRP audits within the MCC system, penalties are applied based on jurisdictional configuration and auditor discretion. Each jurisdiction defines the types of penalties that may be assessed during an audit. These penalty types are configured in the system to reflect the rules and thresholds applicable to that jurisdiction. During the audit process, the auditor is responsible for determining which penalties are appropriate and entering the specific amounts to be charged. This allows for flexibility in enforcement and ensures that penalties are tailored to the circumstances of each audit case. Once entered, the penalties are added to the audit invoice and processed through the system's batch routines, ensuring accurate billing and reporting.
8	**Communication to/from registrants**			
1.)	Ability to upload documentation	YES		The Motor Carrier Connect (MCC) IRP/IFTA system allows registrants to securely upload documentation through the web application. Document upload functionality is available during workflows such as new account setup, renewals, and user account management. The system supports multiple file formats and enforces validation rules to ensure required documents are submitted based on Oklahoma's configuration. Uploaded documents are stored securely and are immediately accessible to authorized state staff for review. All upload actions are tracked through audit logs, and email notifications can be triggered based on submission status or document review outcomes. Refer to Section 07-01 Explore MCC Product Literature, Document Management
2.)	Communication tracking: Capture and maintain the communications within the registrant's file in the system	YES		The Motor Carrier Connect (MCC) IRP/IFTA system includes built-in communication tracking that captures and stores all relevant communications within the registrant's account and audit files. This includes system-generated messages, email notifications, and staff-entered notes or correspondence. Communications are timestamped and associated with specific actions or workflows, such as application submissions, approvals, or document reviews. Authorized users can view the full communication history for each registrant, ensuring transparency and continuity in case management. All entries are governed by security roles and retained according to configurable retention policies. Refer to Section 07-01 Explore MCC Product Literature, Communications / Correspondence Management
3.)	Allow for email and SMS messaging to registrants that complies with confidentiality requirements of OCC	YES		The MCC system currently supports outbound email messaging to registrants. These communications are configurable by jurisdiction, logged within the registrant's file, and designed to comply with OCC confidentiality standards. While SMS messaging is not currently supported, Explore has plans to develop and implement SMS functionality in a future system release to enhance registrant communication options.
4.)	Allow for system notifications to registrants	YES		The MCC IRP/IFTA system delivers system-generated notifications to registrants through both real-time triggers and scheduled batch processes. **Real-time notifications** are automatically generated in response to specific system events, including: - User account requests such as password resets or profile updates - Online application submissions and status changes - Workflow re-assignments initiated by jurisdiction staff These notifications are sent immediately to ensure registrants and staff are informed of critical actions as they occur. **Scheduled batch notifications** are configured to run at defined intervals and support broader communication needs such as renewal reminders, compliance alerts, and informational updates. These are tailored to registrant groups based on criteria such as account status, expiration dates, or transaction history.
9	**Capability to perform records reviews**	YES		The MCC system enables Oklahoma to conduct records reviews as part of its IFTA and IRP audit operations, allowing auditors to examine carrier documentation such as trip logs, fuel receipts, and operational data without initiating a full audit. These reviews are used to verify compliance, identify discrepancies, and determine whether further audit action is needed. Each review is documented with findings and supporting notes, and the system allows secure upload and storage of carrier-provided documents. In accordance with IFTA and IRP audit manuals, MCC applies the "three records reviews equal one audit" conversion when calculating and generating the audit count in the annual audit report. The system also produces a detailed report that includes all audits and records reviews conducted, supporting the jurisdiction's annual audit submission with full transparency and traceability.

10	**Prior and Current year audit capabilities**	YES		The MCC system provides robust capabilities for managing both prior and current year audits under the IRP program. Audits can be initiated for fleets up to three registration years in the past, allowing for comprehensive historical and current compliance reviews. For current year audits, MCC dynamically calculates audit results based on the most recent fleet data. If changes are made to the fleet during the audit period, such as updates weights and vehicles, MCC automatically incorporates those changes into the audit calculations to ensure accuracy. Additionally, once the appeal period concludes, the system performs a final recalculation of the audit to reflect any updates or adjustments made during the appeal. If changes were made and the calculation results differ, the system will allow for the audit to go through another appeal period process. This ensures that the final audit results are complete and accurate before the audit is finalized and sent out for billing. All audits and records reviews, whether from prior or current years, are included in MCC's detailed audit summary report. Refer to Section 07-01 Explore MCC Product Literature, Audit Management.
11	**Financial:** ***** Note: The internal IMS system will be the financial system of record, and an interface will be required.**			
1.)	Billing:			
	i.) Generate assessments per audit results, which will create an invoice in IMS	YES		The MCC system will generate assessments based on finalized audit results and will transmit the resulting invoice directly to the Integrated Management System (IMS). This applies to both IRP and IFTA audits. The assessment includes all applicable fees, penalties, and interest, calculated according to Oklahoma's jurisdictional rules and audit findings. For current year audits, MCC ensures that any changes made to the fleet while the audit is in progress are incorporated into the final calculation. Additionally, the system will perform a final recalculation after the appeal period ends to ensure accuracy before billing. Once the audit is finalized, MCC will automatically generate and transmit the invoice to IMS for carrier notification and payment processing. The system also supports tracking of payment status and late payment eligibility. If the invoice remains unpaid past the configured due date, MCC will apply late payment interest and penalties as defined by Oklahoma's rules. All audit invoices are included in MCC's reporting tools, providing full visibility into audit-related financial activity.
	ii.) Ability to generate reports compliant with state requirements	YES		Explore's MCC IRP/IFTA system includes a wide range of standard financial reports, supports ad hoc reporting, and offers the ability to custom-build reports to meet Oklahoma's specific state requirements. This ensures flexibility in reporting while maintaining compliance with all mandated formats and standards.
	iii.) Ability to report changes in prior period data in the current month of activity	YES		MCC is capable of generating reports that reflect changes to prior period data within the current month's activity.
	iv.) Generate reports which reflect historical data and trends	YES		MCC is capable of generating reports that reflect historical data and trends.
	v.) Ability to incorporate clearinghouse reports	YES		**Clearinghouse Report Support:** MCC offers a variety of clearinghouse reports, including transmittals in PDF format, to support jurisdictional data exchange and compliance tracking. These reports are generated in alignment with IFTA requirements and can be accessed directly within the system for review and audit purposes. **IFTA Return-Level Visibility:** At the individual return level, users can view the exact data that was transmitted to the clearinghouse. This includes jurisdictional tax details, mileage, fuel usage, and financial information. For jurisdictions using Option 1 for transmittals, MCC also displays any remaining financial data that has yet to be sent, ensuring complete visibility into the transmission process. **IFTA Audit-Level Visibility:** Similarly, at the IFTA audit level, MCC provides users with a clear view of the data transmitted to the clearinghouse. This includes audited jurisdictional tax amounts, mileage, fuel usage, and any adjustments resulting from audit findings or supplements. For jurisdictions using Option 1, the system also shows any remaining financial data pending transmission.
	vi.) Potential ability to collect partial payments and provide updated bills with recalculated amounts if allowed by Oklahoma state statute	YES		The MCC IRP/IFTA system supports the potential ability to collect partial payments and generate updated bills with recalculated amounts, if permitted by Oklahoma state statute. When a partial payment is applied to an audit or return invoice, MCC recalculates the remaining balance and adjusts any applicable late payment interest or penalties based on the updated amount and timing of the payment. This ensures that billing remains accurate and compliant with Oklahoma's financial rules. In addition to partial payment handling, MCC also accommodates Payment Plans. If a carrier is enrolled in a payment plan, the system tracks scheduled payments, applies them to outstanding balances, and ensures that late payment interest and penalties are not assessed while the plan is active. MCC maintains full visibility into payment activity and provides updated invoices and reports that reflect the current financial status of each account.
	vii.) Interface with IMS and provide transactional data from invoices including all pass-thru revenue a.) This will be based around the OCC account ID that is generated in the IMS system. The selected system will need to use the OCC account ID as an identifier within the system. 1.) This would require name, address, and phone number be collected for sales of permits. b.) Timing of data transfers will need to be discussed.	YES		Explore's MCC IRP/IFTA system is designed to integrate securely and effectively with external financial systems, including Oklahoma's internal IMS system, which will serve as the financial system of record. **Interface with IMS** Explore will develop and maintain a secure interface that transmits transactional data from invoices, including all pass-through revenue, to the IMS system. This integration ensures that financial records are centralized and consistent with jurisdictional reporting requirements. **Use of OCC Account ID** The MCC system will incorporate the OCC account ID, generated by the IMS system, as a primary identifier for registrants. This ID will be used to associate financial transactions and registrant data across both systems, ensuring alignment and traceability. **Data Collection for Permit Sales** To support accurate financial reporting and integration, the MCC system will collect and transmit the following registrant details for permit sales: - Name - Address - Phone number These data elements will be linked to the OCC account ID and included in the transactional data sent to IMS. **Timing of Data Transfers** Explore will collaborate with Oklahoma's technical and financial teams to define the timing and frequency of data transfers. The system supports both real-time and scheduled batch processing, allowing flexibility based on operational and reporting needs. **Audit and Reconciliation** All financial transactions processed through MCC will be logged, auditable, and reconciled against IMS records. Explore will support reconciliation processes and provide detailed transaction histories as needed. **Collaboration and Testing** Explore will work closely with Oklahoma's team to define interface specifications, conduct integration testing, and validate data flows prior to production deployment.

	viii.) Provide information required to IMS to generate refunds for overpayments	YES		We have successfully implemented numerous financial interfaces that transmit detailed financial information, including refund data for overpayments. MCC supports providing the necessary information to IMS to initiate and process refunds, ensuring accurate reconciliation and alignment with jurisdictional financial workflows.
	ix.) Ability to make corrections in the system to fix billing errors	YES		MCC allows authorized users to make corrections in the system to resolve billing errors through secure, task-driven workflows. One method includes adjusting fees either upward or downward, based on the nature of the correction and the user's assigned security permissions. In some instances, billing errors can be corrected by voiding the invoice. This is done by unfiling the transaction, making the necessary updates, and then refiling the application, which generates a new invoice with the corrected fee structure. All changes are tracked for audit purposes, ensuring transparency, accuracy, and compliance with financial controls.
	x.) Interface with the payment processing system	YES		MCC supports integration with external payment processing systems to enable secure and efficient financial transactions. The system interfaces with third-party payment platforms to handle real-time authorization, settlement, and confirmation of payments. This allows registrants to pay using supported methods such as credit card, ACH, or other jurisdiction-approved options. Importantly, the contractual relationship with the third-party payment processor is between the vendor and the state, not Explore. Explore facilitates the technical integration and ensures that payment data is securely transmitted, properly logged, and reflected in the registrant's account and application status. The interface is configured and tested in collaboration with the jurisdiction to meet financial and security standards.
	xi.) Identify and maintain required payment types according to payment methods approved by agency rules a.) ACH – payment through QuickPay	YES		Explore's MCC IRP/IFTA system supports the identification and management of payment types in accordance with agency-approved methods and rules. The system allows jurisdictions to define and enforce accepted payment types, including ACH payments through QuickPay, as specified. Logic can be configured to provide warnings or restrictions for payment methods that require special handling. For example, if a registrant selects check as a payment method, the system can display a warning indicating that only certified funds are accepted, in compliance with agency rules.
	xii.) Printed billing documents must contain a barcode supplied by IMS	YES		At present, the Motor Carrier Connect (MCC) system does not include barcodes on printed billing documents. However, Explore is fully committed to meeting this requirement and will work collaboratively with the Oklahoma Corporation Commission (OCC) to implement barcode functionality in alignment with IMS specifications. Explore will engage with OCC to gather the necessary technical requirements and ensure that barcodes provided by IMS are accurately incorporated into all relevant billing documents. This enhancement will be delivered through custom development and tested thoroughly to ensure compatibility, accuracy, and compliance with OCC's financial processing standards.
	xiii.) Printed billing documents must contain a barcode supplied by IMS	YES		See Above.
12	**Reports**			
1.)	Ability to generate reports compliant with state requirements	YES		Explore's MCC IRP/IFTA system includes a wide range of standard financial reports, supports ad hoc reporting, and offers the ability to custom-build reports to meet Oklahoma's specific state requirements. This ensures flexibility in reporting while maintaining compliance with all mandated formats and standards.
2.)	Ability to report changes in prior period data in the current month of activity	YES		MCC is capable of generating reports that reflect changes to prior period data within the current month's activity.
3.)	Generate reports which reflect historical data and trends	YES		MCC is capable of generating reports that reflect historical data and trends.
IV	**Trip and Fuel Permits**			
	Provide the following functionality (digitally):			
1	**Submit new applications**			
1.)	IRP Trip Permit	YES		The MCC system includes built-in functionality for issuing and managing IRP Trip Permits. Oklahoma users can create, file, pay for, and track these permits directly within the system. The workflow is fully integrated, with configurable fields, validations, and expiration rules. Internal users access the permit creation through the Permit Maintenance interface, while external users can initiate requests via a public-facing portal. All IRP Trip Permit activity is stored and reportable within MCC.
2.)	IFTA Fuel Permit	YES		IFTA Fuel Permits are fully supported within the MCC system. Oklahoma users can create and manage these permits using the same integrated workflow as other permit types. The system includes validations for vehicle weight and jurisdictional travel, and supports both internal and external access for permit creation and payment. Permit duration and expiration logic are configurable, and all issued permits are tracked and reportable within MCC.
3.)	Unladen Permit (Hunters Permit)	YES		Unladen Permits, also known as Hunter's Permits, are built into the MCC system and available for issuance and management by Oklahoma users. The system supports full permit lifecycle management, including creation, filing, payment, and tracking. These permits follow the same workflow and validation structure as other trip permits, ensuring consistency and compliance with jurisdictional rules.
2	**Financial:** ***** Note: The internal IMS system will be the financial system of record, and an interface will be required.**			
1.)	Billing:			
	i.) Upon purchase of a temporary permit, it will create an invoice and a receipt in IMS	YES		Upon the purchase of a temporary permit, the Motor Carrier Connect (MCC) system generates the invoice and receipt internally. The system is designed to interface seamlessly with the Integrated Management System (IMS), enabling the transmission of both the invoice and receipt data to IMS. This integration ensures that financial records are synchronized across platforms, allowing IMS to maintain accurate documentation and provide users with confirmation of payment through its own channels.

	ii.) Ability to generate reports compliant with state requirements	YES		Explore's MCC IRP/IFTA system includes a wide range of standard financial reports, supports ad hoc reporting, and offers the ability to custom-build reports to meet Oklahoma's specific state requirements. This ensures flexibility in reporting while maintaining compliance with all mandated formats and standards.
	iii.) Ability to report changes in prior period data in the current month of activity	YES		MCC is capable of generating reports that reflect changes to prior period data within the current month's activity.
	iv.) Generate reports which reflect historical data and trends	YES		MCC is capable of generating reports that reflect historical data and trends.
	v.) Ability to incorporate clearinghouse reports	YES		The Motor Carrier Connect (MCC) system currently does not transmit trip permit information to the clearinghouse. However, the system is designed with flexibility to accommodate future regulatory requirements. If transmission of trip permit data to the clearinghouse becomes mandated, MCC will be enhanced accordingly to ensure full compliance. This approach supports a scalable and forward-compatible architecture, allowing the system to evolve in alignment with industry standards and jurisdictional needs.
	vi.) Interface with IMS and provide transactional data from invoices including all pass-thru revenue a.) This will be based around the OCC account ID that is generated in the IMS system. The selected system will need to use the OCC account ID as an identifier within the system. 1.) This would require name, address, and phone number be collected for sales of permits. b.) Timing of data transfers will need to be discussed.	YES		Explore's MCC IRP/IFTA system is designed to integrate securely and effectively with external financial systems, including Oklahoma's internal IMS system, which will serve as the financial system of record. **Interface with IMS** Explore will develop and maintain a secure interface that transmits transactional data from invoices, including all pass-through revenue, to the IMS system. This integration ensures that financial records are centralized and consistent with jurisdictional reporting requirements. **Use of OCC Account ID** The MCC system will incorporate the OCC account ID, generated by the IMS system, as a primary identifier for registrants. This ID will be used to associate financial transactions and registrant data across both systems, ensuring alignment and traceability. **Data Collection for Permit Sales** To support accurate financial reporting and integration, the MCC system will collect and transmit the following registrant details for permit sales: - Name - Address - Phone number These data elements will be linked to the OCC account ID and included in the transactional data sent to IMS. **Timing of Data Transfers** Explore will collaborate with Oklahoma's technical and financial teams to define the timing and frequency of data transfers. The system supports both real-time and scheduled batch processing, allowing flexibility based on operational and reporting needs. **Audit and Reconciliation** All financial transactions processed through MCC will be logged, auditable, and reconciled against IMS records. Explore will support reconciliation processes and provide detailed transaction histories as needed. **Collaboration and Testing** Explore will work closely with Oklahoma's team to define interface specifications, conduct integration testing, and validate data flows prior to production deployment.
	vii.) No refunds except in case of a system error	YES		
	viii.) Interface with the payment processing system	YES		MCC supports integration with external payment processing systems to enable secure and efficient financial transactions. The system interfaces with third-party payment platforms to handle real-time authorization, settlement, and confirmation of payments. This allows registrants to pay using supported methods such as credit card, ACH, or other jurisdiction-approved options. Importantly, the contractual relationship with the third-party payment processor is between the vendor and the state, not Explore. Explore facilitates the technical integration and ensures that payment data is securely transmitted, properly logged, and reflected in the registrant's account and application status. The interface is configured and tested in collaboration with the jurisdiction to meet financial and security standards.
	ix.) Identify and maintain required payment types according to payment methods approved by agency rules a.) ACH – payment through New NIC Payment portal	YES		The Explore MCC IRP/IFTA system supports the identification and management of payment types in accordance with agency-approved methods and rules. Jurisdictions can configure and maintain accepted payment types within the system, including ACH payments processed through the New NIC Payment Portal. The system is designed to enforce payment method policies, ensuring compliance with agency-specific requirements. For instance, if a registrant selects a payment method that requires special handling—such as a check—the system can be configured to display a warning or restrict the option, indicating that only certified funds are accepted. This flexible configuration ensures secure, compliant, and jurisdictionally aligned payment processing.
	x.) (Potential) Ability to block customers who are in dispute with the agency (using payor information from NIC) (a.)Reflect adjustments in the reports based on credit card disputes or ACH returns	YES		The Explore MCC IRP/IFTA system is designed with the flexibility to incorporate enhanced payment monitoring and enforcement capabilities. If required, the system can be configured to interface with the NIC Payment Portal to identify customers who are in dispute with the agency, using payor information such as credit card chargebacks or ACH returns. Based on this data, MCC can support the ability to block or restrict access for those customers until the dispute is resolved. Additionally, the system can reflect adjustments in financial reports to account for disputed transactions, ensuring accurate reconciliation and compliance with agency financial policies.
3	**Bulk Permits**			
1.)	Approved vendor requests block of permit numbers via paper request in the mail with payment attached (using approved payment methods). (Potential – make this an electronic request/payment)	YES		Approved Vendor Requests via Mail: MCC can support the current process where approved vendors request blocks of permit numbers via paper mail with payment attached. The system allows internal users to create block permits manually and associate them with the requesting agency. MCC is capable of supporting an electronic workflow for block permit requests and payments. Jurisdictions can configure external access for approved vendors to submit requests and make payments online, streamlining the process and reducing manual handling.
2.)	Block of permit numbers sent out to approved vendor electronically	YES		Once a block permit is created, MCC allows for the electronic transmission of individual permit numbers to the approved vendor. Each permit within the block is tracked and can be viewed, assigned, and managed through the system.
3.)	Approved vendor notifies OCC when permits are sold to allow for tracking of permit sales against the number of permits in the block via daily uploads of total daily sales.	YES		The MCC system currently supports the tracking of block permit sales for approved vendors, with individual permit statuses entered manually by internal users. To meet Oklahoma's requirement for daily reporting of permit sales, the system will be enhanced to allow vendors to upload a file that updates the status of each permit within the block. This enhancement will streamline the process, reduce manual data entry, and improve accuracy in tracking sold and remaining permits.

4	**Reports**			
1.)	Both individual permits and bulk permits together in one report	YES		The Explore MCC IRP/IFTA system supports comprehensive reporting capabilities, including the ability to generate reports that consolidate both individual and bulk permit transactions. This unified reporting approach ensures that agencies can view and analyze all permit activity in a single report, streamlining oversight and reconciliation processes.
2.)	Any other reports deemed necessary for the agency, state, feds, etc.	YES		The Explore MCC IRP/IFTA system includes a variety of standard (canned) reports designed to meet common operational and compliance needs. In addition to these built-in reports, the system supports ad hoc reporting capabilities, allowing users to generate customized reports based on specific OCC requirements. Explore will work collaboratively with OCC to develop new reports as needed, ensuring that all reporting needs, whether for agency use, state-level oversight, or federal compliance, are effectively supported.
V	**Comply with Performance Registration Information Systems Management (PRISM) requirements and functionality**	YES		The Explore MCC IRP/IFTA system is fully capable of complying with Performance Registration Information Systems Management (PRISM) requirements and functionality. In addition to supporting registration holds for carriers under federal out-of-service orders and linking safety performance data to motor carrier records, MCC includes an interactive API integration with PRISM. This allows for live inquiries to retrieve the most current carrier safety and registration data directly from PRISM, ensuring real-time validation and compliance. This dynamic connection enhances the accuracy and responsiveness of the registration process while supporting federal safety oversight.
1	**Reports – standard reports**	YES		The Explore MCC IRP/IFTA system includes a set of standard reports that support compliance with PRISM requirements. These reports provide visibility into carrier safety status, registration holds, and MCSIP participation, and are designed to assist jurisdictions in monitoring and enforcing federal safety mandates. The system's reporting capabilities include summaries of carriers under out-of-service orders, USDOT number validation results, and registration activity linked to safety performance. These standard reports are available on demand and can be customized or expanded in collaboration with OCC to meet evolving PRISM reporting needs.
2	**API connections**	YES		The Explore MCC IRP/IFTA system includes a robust API integration with the PRISM program, enabling real-time connectivity for carrier safety and registration validation. Through this interactive API, MCC can perform live inquiries to PRISM, retrieving the most current data related to USDOT numbers, MCSIP status, and out-of-service orders. This connection ensures that registration decisions are based on up-to-date federal safety information and supports automated enforcement of PRISM-related requirements. The API also facilitates seamless data exchange between MCC and PRISM, enhancing accuracy, compliance, and operational efficiency.
VI	**Comply with Oklahoma State Requirements**			
1	**Interface with:**			
1.)	State and agency systems			
	i.) Secretary of State Withholding	YES		The Explore MCC IRP/IFTA system is capable of interfacing with state and agency systems to support business rules related to Secretary of State Withholding. This includes the ability to receive and process data indicating when a registrant is subject to withholding due to non-compliance or outstanding obligations. The system can enforce registration restrictions based on this information, preventing issuance or renewal of credentials until the withholding is resolved. Integration with the Secretary of State's system ensures that MCC maintains alignment with state-level compliance requirements and supports automated enforcement of withholding actions.
	ii.) Service OK OneLink (a) Title Numbers (b) Title Dates (c) Registration History (d) Title Holds	YES		The Explore MCC IRP/IFTA system is capable of interfacing with Service OK OneLink to support key registration functions. This integration allows MCC to access and utilize critical data elements such as title numbers, title dates, registration history, and title holds. These data points play an important role in validating vehicle ownership, identifying registration eligibility, and enforcing title-related restrictions during the registration process. By leveraging real-time or scheduled data exchange with OneLink, MCC ensures accurate and compliant registration workflows aligned with agency requirements.
	iii.) OLETS	YES		The Explore MCC IRP/IFTA system is capable of interfacing with law enforcement data systems such as the Oklahoma Law Enforcement Telecommunications System (OLETS). This integration can support verification of vehicle and registrant information, enforcement of registration holds, and validation of law enforcement-related flags during the registration process. By connecting with OLETS, MCC can enhance compliance, support public safety initiatives, and ensure that registration activities align with state law enforcement protocols.
	iv.) Iteris Commercial Vehicle Information Exchange Window (CVIEW) (IFTA/IRP sends T files to this vendor and then the vendor sends only what is needed to IDR – potentially a SFTP site)	YES		The Explore MCC IRP/IFTA system interfaces with the Iteris Commercial Vehicle Information Exchange Window (CVIEW) for all Explore customers. As part of this integration, the system transmits T files for IFTA and IDR files for IRP to CVIEW. CVIEW then filters and forwards only the necessary data to the appropriate federal repositories, typically via a secure SFTP site. Explore has extensive experience managing this interface, ensuring consistent, compliant, and secure data exchange across jurisdictions.
	v.) Laserfiche (bidirectional data exchange) - agency document management system	YES		The Explore MCC IRP/IFTA system supports bidirectional data exchange with Laserfiche, the agency's document management system. This integration enables MCC to send and retrieve documents and metadata seamlessly, supporting workflows such as permit processing, audit documentation, and registration record management. By leveraging Laserfiche's capabilities, MCC ensures that all relevant documents are securely stored, easily accessible, and properly linked to motor carrier records. The bidirectional interface enhances operational efficiency and supports compliance with agency documentation standards.
	vi.) CC Merchant Account	YES		The Explore MCC IRP/IFTA system integrates with credit card merchant accounts using ePay interfaces to facilitate secure online payments. When a registrant selects credit card as the payment method, the system redirects the user to the designated payment processor's website, where they enter their account information and submit payment. Upon completion, the payment processor returns a success or failure status to MCC. If the payment is successful, MCC automatically updates the associated invoice as paid, ensuring accurate financial tracking and compliance with agency payment processing rules.
	vii.) IMS (OCC Finance)	YES		The Explore MCC IRP/IFTA system is designed to interface with the Integrated Management System (IMS), managed by OCC Finance, to support accurate financial tracking and reconciliation. For example, when users file tax returns or pay invoices through MCC, the system transmits the relevant invoice and receipt data to IMS to ensure centralized financial oversight. Explore has extensive experience and a strong track record of success implementing financial interfaces across multiple jurisdictions. We will work closely with OCC to understand specific requirements and collaborate on the design and implementation of this integration, ensuring full compliance with agency financial protocols and operational needs.

2.)	Federal Systems			
	i.) Performance Registration Information Systems Management (a.) (PRISM)	YES		The Explore MCC IRP/IFTA system has PRISM integration fully enabled to support federal safety compliance and registration enforcement. This includes functionality to identify carriers under federal out-of-service orders, enforce registration holds, and link motor carrier records to safety performance data. The system also features an interactive API connection with PRISM, allowing for real-time inquiries to retrieve the most current carrier safety and registration status. Explore has extensive experience implementing and maintaining PRISM interfaces and will continue working closely with OCC to ensure the integration remains aligned with all federal and agency-specific requirements.
	ii.) UCR (Potential)	YES		The Explore MCC IRP/IFTA system includes plans to implement an interface with the Unified Carrier Registration (UCR) system as part of our development roadmap for this year. While OCC has identified this integration as optional, Explore is committed to delivering this functionality and will configure the UCR interface specifically to meet OCC's requirements. This planned enhancement will support automated validation and data exchange with the UCR system, improving registration accuracy and streamlining compliance workflows.
3.)	Compact			
	i.) IDR Clearinghouse	YES		The Motor Carrier Connect (MCC) system complies with the IDR Clearinghouse requirements by supporting secure, standardized data exchange protocols that align with federal and state interoperability mandates. MCC integrates with the IDR Clearinghouse to: - Transmit and receive carrier registration and credentialing data in accordance with IRP/IFTA standards. - Ensure real-time synchronization of carrier information across jurisdictions to support enforcement and audit activities. - Maintain data integrity and confidentiality through encrypted communication channels and role-based access controls. - Support automated reporting and reconciliation processes to streamline compliance with federal clearinghouse requirements.
	ii.) IFTA Clearinghouse	YES		The Motor Carrier Connect (MCC) system is fully compliant with the IFTA Clearinghouse requirements, supporting both daily transmittals and demographic data exchanges as outlined by the International Fuel Tax Agreement standards. **Daily Transmittals** MCC automates the generation and submission of daily transmittals to the IFTA Clearinghouse. These include: - Jurisdictional registration updates - Account status changes - Credential issuance and renewals - Fuel tax license modifications Transmittals are securely transmitted using standardized formats and protocols, ensuring timely and accurate data synchronization across participating jurisdictions. **Demographic Data** MCC maintains and shares comprehensive carrier demographic data with the Clearinghouse, including: - Legal and DBA names - Physical and mailing addresses - Contact information - Account identifiers and status Demographic updates are pushed daily to ensure consistency and support enforcement, audit, and compliance activities across jurisdictions.
4.)	Compact			
	i.) JP Morgan	YES		The Motor Carrier Connect (MCC) system can fully comply with integration to the JP Morgan payment processor. We have extensive experience implementing electronic payment solutions across multiple jurisdictions. Our standard approach assumes that users are redirected to the JP Morgan-hosted payment portal to securely enter their banking information. Upon confirmation of a successful transaction, MCC automatically marks the associated invoice as paid.
	ii.) S&P Global Mobility (formerly R. L. Polk) - Data resale; contract renewed annually; receives a portion of the IDR files	YES		The Motor Carrier Connect (MCC) system will be able to comply with the interface requirements for S&P Global Mobility. MCC can support the secure extraction and delivery of designated portions of the IDR files for data resale purposes, in accordance with the terms of the annually renewed contract. The system is capable of managing scheduled data transfers and ensuring compliance with all applicable data-sharing and privacy policies.
2	**Comply with all Oklahoma Management Enterprise Services (OMES) technical requirements related to:**			
1.)	Network	YES		Refer to Section 07-02 - Explore - Network
2.)	Security	YES		Refer to Section 07-03 - Explore - Security and Data Protection
3.)	Data	YES		Refer to Section 07-03 - Explore - Security and Data Protection
4.)	Development Approach	YES		Refer to Section 07-04 - Explore - Development Approach
5.)	Documentation and Training	YES		Refer to Section 07-05 - Explore - Documentation and Training
6.)	.			
7.)	Etc.			
8.)	Preference to SaaS and hosted cloud solution	YES		Refer to Section 07-06 - Explore - Hosted Solution

VII	**Minimum Required Experience**			
1	**The supplier must have at least three years' prior experience in working on projects similar in size, scope, technical requirements, and function of the Oklahoma Corporation Commission.**	YES		Refer to Section 07-07 - Explore - Experience
1.)	The supplier must submit documentation demonstrating previous successful experience with at least three such programs. To substantiate the supplier's successful completion of similar programs, appropriate contact names, current telephone numbers, and e-mail addresses must be included in the proposal.	YES		Refer to Section 07-07 - Explore - Experience
	i.) The Program Manager, the main point of contact withOCC, will oversee and be responsible for all aspects of the project. The Program Manager must have at least three years of experience with projects of similar scope and size. The Program Manager will be committed to the project throughout its duration. At least three references from individuals in states or agencies where the proposed program manager has coordinated a comparable assessment program must be provided. It is critical, and required, that the manager have sufficient authority within the company to obtain cooperation from all sections and to arrange priority for the Oklahoma project when necessary.	YES		Refer to Section 07-07 - Explore - Experience
7.9	**Any other additional Value-Added services**			

Section Seven: Explore Proposed Solution

Technical Architecture

Motor Carrier Connect (MCC) is built on a robust, multi-tier technical architecture that emphasizes scalability, security, and maintainability. The system leverages a modular design with clearly defined layers, presentation, application, integration, and data, to support jurisdiction-specific configurations and seamless interoperability. It incorporates industry-standard protocols, modern development frameworks, and secure hosting infrastructure to ensure high availability, performance, and long-term sustainability.

Architecture & Technology Stack

Software Architecture:

- **Presentation Layer:** Built using modern web standards to ensure responsive design and accessibility.
- **Application Layer:** Modular services configured to meet jurisdiction-specific requirements.
- **Integration Layer:** Interfaces with external systems such as federal agencies and payment processors using secure protocols.
- **Data Layer:** Supports structured and unstructured data, with comprehensive audit logging capabilities.

Hardware & Hosting:

- Hosted in a secure, virtualized infrastructure with load-balanced tiers for web, application, and database services.
- Primary hosting is in a high-security data center with redundancy and environmental controls.
- Disaster recovery is supported through a geographically separate enterprise-grade facility.
- Infrastructure is optimized for performance, scalability, and availability.
- System monitoring is performed using enterprise-grade tools to ensure uptime and security.

Network & Security:

- Encrypted communication using current TLS standards.
- Enterprise-grade firewalls and VPNs protect network boundaries.
- Real-time monitoring, intrusion detection, and secure API gateways are in place.
- Encryption standards and patching policies align with federal compliance requirements.
- Access control is enforced through role-based permissions and multi-factor authentication.

System Features & Capabilities

- **Scalability**: Horizontal/vertical scaling, dynamic resource allocation, CI/CD pipelines
- **Extensibility**: Modular add-ons, customizable workflows

Internal

- **Integration**: RESTful APIs, XML/JSON/EDI standards
- **Data Management**: Migration tools, validation, historical access
- **Reporting**: Ad hoc and scheduled reports, data extracts
- **Usability**: WCAG 2.1 compliance, embedded help, sandbox training
- **Interoperability**: Standard formats (CSV, Excel, PDF), secure messaging, middleware
- **Maintainability**: Modular design, automated deployment, real-time monitoring

Key Benefits of the MCC Architecture

The MCC system's technical architecture is designed to deliver operational excellence across multiple dimensions. Its modular, scalable, and secure design supports jurisdictional flexibility and long-term sustainability. Key benefits include:

- **Scalability:** Load balancing, high availability SQL configurations, and dynamic resource allocation ensure the system can grow with demand.
- **Adaptability:** Modular frameworks and automated build pipelines support rapid configuration and deployment across jurisdictions.
- **Interoperability:** Support for standard data formats (CSV, Excel, PDF), secure messaging protocols, and middleware integration enables seamless connectivity with external systems.
- **Security & Compliance:** Network segmentation, encryption standards, and multi-tier firewalls provide robust protection and alignment with regulatory requirements.
- **Maintainability:** A modular design, automated deployment processes, and real-time monitoring tools simplify ongoing system management and reduce operational overhead.

Access & End-User Requirements

MCC is accessible via modern web browsers (Chrome, Firefox, Safari, Edge) with no special installation required. End-point devices should support:

- Microsoft Excel (audit file handling)
- Microsoft Word (account correspondence)
- PDF viewer (standard browser support)

Programming Languages

Programming languages used for development, configuration, and customization:

- **Frontend:** .NET Core, HTML, CSS, JavaScript, JQuery
- **Backend:** C# on .NET Framework
- **Database:** SQL Server
- **Core Software:** Originally developed in 2002; major modernization completed in 2021

Proprietary Components and COTS Architecture

While MCC incorporates open-source technologies to enhance functionality and maintain modern development standards, its core application logic, business rules engine, and workflow

Internal

orchestration components are proprietary. These elements are not available as open-source or third-party licensed software and are maintained exclusively to ensure alignment with jurisdictional requirements and ongoing compliance standards.

Proprietary components include:

- Custom-developed middleware that manages communication between the frontend, backend, and database layers
- Business logic modules supporting IRP, IFTA, Permitting, and Intrastate Operating Authority workflows
- Internal tools and utilities used for deployment, configuration, and system management

The Explore MCC system is delivered as a fully hosted solution, meaning that all hardware infrastructure is managed by Explore Information Services, LLC. The system is deployed in a multi-tier architecture across dedicated web, application (middle tier), and database servers, each optimized for performance, scalability, and security. Refer to **Section 07 – Explore – Hosted Solution** for additional information.

Release Management and Enhancement Strategy

The MCC system follows a structured release cadence to ensure continuous improvement, compliance alignment, and system stability. On average, four major releases are deployed annually, each containing a mix of enhancements, maintenance updates, and jurisdictional compliance changes. In addition, minor, targeted releases are issued throughout the year to address urgent fixes, evolving jurisdictional priorities, and regulatory mandates.

Over the past three years, MCC has consistently delivered:

- Four major releases per year, each including enhancements, bug fixes, and compliance updates
- Multiple minor releases aligned with jurisdictional deadlines or urgent needs
- A predictable release cadence that supports timely delivery while maintaining platform stability

Release content is driven by a combination of:

- Required maintenance and security updates
- Jurisdictional compliance mandates
- User feedback and enhancement requests
- Internal roadmap priorities and backlog grooming

Explore collaborates closely with jurisdictional stakeholders to prioritize and validate release content, ensuring that updates are relevant, timely, and aligned with operational needs.

MCC is a multi-tenant system built on a shared codebase. Enhancements developed for specific jurisdictions are typically incorporated into the core platform and made configurable. This allows

Internal

jurisdictions to enable or disable features based on their operational requirements without duplicating code or compromising system integrity.

Recent roadmap enhancements include:

- Enhanced IFTA reporting with transmission details to the IFTA Clearinghouse
- Web-based reports for email logging
- Dashboard improvements (e.g., new widgets, Required Materials, pending address changes)
- Fuel schedule summary enhancements for amended returns
- User-entered reasons for amended returns
- Pending status workflows for carrier/agent address changes requiring state review
- Online application enhancements
- Reverse IRP refund functionality (vehicle credits)
- Migration of IRP delinquency processes to the cycle processor

Each release is supported throughout the life of the client's contract. Explore provides:

- Ongoing maintenance, issue resolution, and enhancement support
- Detailed release notes for each deployment, including all items moved to the target environment and any known issues
- Draft release notes reviewed with clients prior to production deployment
- Notes for both QA and production environments to support informed testing and planning

All release components are deployed system-wide across jurisdictions using MCC, ensuring consistency and platform-wide stability. However, MCC's modular architecture allows jurisdictions to adopt new capabilities at their own pace. Features can be selectively enabled or disabled without impacting overall system functionality, providing flexibility while preserving performance and integrity.

Data Exchange, Interfaces, and Migration Capabilities

Flexible and Secure Data Exchange

MCC is designed to support flexible, secure, and standards-compliant data exchange across jurisdictions. The system includes robust tools for interfacing with external systems and managing historical data migration, ensuring seamless integration and operational continuity.

Explore MCC supports multiple interface mechanisms:

- SFTP (Secure File Transfer Protocol) for secure file exchange
- Flat file generation for batch exports (e.g., IFTA transmittals, decals, demographic data)
- Secure APIs protected by client certificates, IP restrictions, and encrypted credentials
- SQL Server Management Studio and DTS tools for direct database interactions during setup and migration

Interface formats include:

- XML for structured, machine-readable data (e.g., Upload IFTA returns)
- JSON for systems supporting modern web-based data exchange (e.g., electronic payment platforms)
- CSV for tabular data exchange
- Flat files for batch processing and clearinghouse submissions

MCC supports both interactive and batch interfaces:

- Online APIs and web services for real-time interactions (e.g., electronic payments, PRISM API)
- Scheduled batch interfaces for systems like IFTA Clearinghouse and custom state integrations

All interfaces are treated as configurable components. Formats, triggers, transmission rules, and file naming conventions can be tailored per jurisdiction. MCC adheres strictly to standard layouts defined by external entities such as IRP Inc., IFTA Inc., and PRISM, while also supporting jurisdiction-defined formats through collaborative design and implementation.

Interface Scheduling and Execution

MCC supports flexible and robust scheduling options for initiating interfaces and batch processes. Scheduling configurations are tailored to meet jurisdiction-specific timing, frequency, and operational requirements. There are no hard constraints on batch timing; however, schedules are optimized to avoid system load conflicts and ensure consistent performance.

Data Migration Capabilities

Explore has extensive experience successfully migrating IRP and IFTA data across multiple jurisdictions. Our team has led numerous implementations involving the conversion of complex legacy datasets into the MCC platform, ensuring data integrity, operational continuity, and compliance readiness. Whether migrating full historical records or targeted data sets, Explore applies proven methodologies tailored to each jurisdiction’s requirements. This includes mapping legacy data to MCC structures, validating key data elements, and reconciling records to support fee calculations, credentialing, audit history, and outstanding invoice tracking. Our flexible approach ensures jurisdictions retain the data necessary for operations and compliance, while minimizing disruption and complexity.

Explore’s data migration approach focuses on:

- Migrating all key data elements required for fee/tax calculations and credential printing
- Preserving audit history, registration credentials, and outstanding invoice tracking
- Ensuring data integrity through validation and reconciliation processes

In cases where detailed audit case data cannot be extracted from legacy systems, Explore converts high-level audit indicators to reflect prior audit activity. This ensures jurisdictions retain necessary compliance and operational data without introducing unnecessary complexity.

Internal

Typically, 5 to 7 years of historical data are converted, based on jurisdictional needs. Explore assists clients by:

- Reviewing statutory retention requirements
- Assessing relevance of historical data for ongoing operations
- Conducting stakeholder interviews to understand user needs
- Performing legacy-to-MCC data mapping and volume analysis

Both automated and manual conversion methods are supported, with validation performed throughout the process to ensure completeness and accuracy.

Internal

Section Seven: Explore Security and Data Protection

Explore Information Services, LLC is committed to delivering a secure, resilient, and compliant MCC IRP/IFTA system that protects sensitive data, supports jurisdictional requirements, and aligns with federal and industry-recognized standards. Our security posture is built on a foundation of continuous improvement, transparency, and multi-layered defense mechanisms that span infrastructure, application, and operational domains.

While we recognize the importance of aligning with customer-specific security policies, we maintain a unified security framework to ensure consistent protection across all client environments. This approach ensures that no individual customer's requirements compromise the integrity or safety of another's data.

System Security

Explore acknowledges the importance of aligning with federal cybersecurity frameworks, particularly NIST SP 800-171, which governs the protection of Controlled Unclassified Information (CUI) in non-federal systems. While the MCC IRP/IFTA system is not currently certified as fully compliant with NIST SP 800-171, Explore maintains a strong security posture through its SOC 2 Type 2 compliance, which includes many controls that directly map to NIST SP 800-171 Rev. 3.

Explore undergoes annual SOC 2 audits that evaluate the effectiveness of security controls across the MCC application and hosting environment. These audits cover key domains such as:

- Access control
- Audit and accountability
- Configuration management
- Identification and authentication
- Incident response
- System and communications protection
- System and information integrity

Explore has conducted internal mapping exercises to demonstrate alignment between SOC 2 and NIST SP 800-171 requirements. This mapping confirms that our existing security framework substantially supports the objectives of NIST, even though formal certification has not yet been pursued. We continue to monitor updates to NIST guidance and incorporate relevant controls into our security roadmap. Should Oklahoma Corporation Commission require formal NIST SP 800-171 compliance, Explore is prepared to support a collaborative gap assessment and provide input toward a remediation strategy, as appropriate.

Identity and Access Management

Explore recognizes that secure digital identity management is critical to protecting access to sensitive systems and data. While the MCC IRP/IFTA system is not formally certified against NIST SP

Internal

800-63, its identity and access management framework is designed to align with the principles and assurance levels outlined in the guideline.

Key identity-related controls include:

- **Multi-Factor Authentication (MFA)**: MCC supports MFA for all user accounts. Activation is jurisdiction-controlled and must be explicitly requested. When enabled, MFA aligns with Identity Assurance Level 2 (IAL2) and Authenticator Assurance Level 2 (AAL2).
- **Role-Based Access Control (RBAC)**: Access to system functions and data is governed by RBAC policies, ensuring users only access resources appropriate to their roles.
- **Session Management**: Sessions are monitored and automatically terminated after periods of inactivity to reduce risk of unauthorized access.
- **Credential Management**: Password policies enforce complexity, expiration, and reuse restrictions consistent with NIST SP 800-63B guidelines.
- **Audit Logging**: Authentication events are logged and monitored to detect anomalies and support incident response.

Explore continues to enhance its identity management practices to align with evolving federal standards.

Vulnerability Management and Security Testing

Explore maintains a comprehensive vulnerability management program that follows industry-recognized best practices, many of which are derived from NIST SP 800-115. The MCC IRP/IFTA system undergoes regular security testing and assessment activities that align with the principles outlined in this guideline.

Key practices include:

- Automated vulnerability scanning of infrastructure and application components using industry-standard tools.
- Manual penetration testing performed by third-party security experts on a scheduled basis or during major system updates.
- Security configuration reviews to ensure systems are hardened according to best practices.
- Patch management processes ensure timely remediation of identified vulnerabilities.
- Audit logging and monitoring to detect and respond to anomalous activity.

These activities are documented and reviewed as part of Explore's annual SOC 2 Type 2 audit. While formal certification against NIST SP 800-115 is not currently held, our testing and assessment practices are designed to meet or exceed the intent of the guideline.

Non-Repudiation Controls

To ensure that users cannot deny their actions within the MCC system, Explore has implemented a combination of technical and procedural controls that support non-repudiation:

- **Audit Logging**: All user interactions are logged with timestamps, user IDs, IP addresses, and specific actions. Logs are immutable and retained according to policy.

- **User Authentication**: Unique credentials are required for access. MFA, when enabled, strengthens identity verification.
- **Digital Signatures and Confirmations**: Key transactions generate confirmation records and transaction IDs that serve as digital evidence.
- **RBAC Enforcement**: Actions are restricted based on user roles, ensuring accountability.
- **Secure Transmission Protocols**: All data is encrypted using HTTPS/TLS to ensure integrity and authenticity.

These mechanisms ensure that all interactions are traceable, verifiable, and attributable to specific users.

Intrusion Detection and Response

Explore employs a robust Endpoint Detection and Response (EDR) solution across its infrastructure to detect, record, and respond to unauthorized access attempts or system modifications.

Key features include:

- **Real-Time Monitoring and Logging**: Continuous monitoring of system activity, including process execution, file access, and network connections.
- **Behavioral Analysis and Alerting**: Suspicious behavior triggers automated alerts.
- **Network Operations Center (NOC) Response**: Alerts are routed to Explore’s NOC team for investigation and remediation.
- **Audit Trail and Forensics**: All events are recorded to support forensic analysis and compliance reporting.

This layered approach ensures timely detection and response to threats, maintaining system integrity.

Data Privacy and Protection

Explore has implemented a combination of technical and organizational measures to ensure the privacy and protection of confidential data and sensitive communications throughout their lifecycle.

Key safeguards include:

- **Data Encryption**: HTTPS with TLS 1.2 is used for securing data in transit. Data at rest is encrypted using SQL Server’s native encryption capabilities, which comply with FIPS 140-2 standards.
- **Access Controls**: Role-Based Access Control (RBAC) ensures only authorized users can access specific data and system functions.
- **PII Masking**: Personally Identifiable Information (PII) fields are masked across all production environments. Viewing unmasked data is strictly controlled through RBAC permissions.
- **Multi-Factor Authentication (MFA)**: Adds an extra layer of protection when enabled.

Internal

- **Secure Hosting Environment**: SOC 2 Type 2-compliant infrastructure with robust physical and network security controls.
- **Data Minimization and Retention Policies**: Data is retained only as long as necessary to meet operational and regulatory requirements.
- **Privacy Awareness and Training**: All personnel receive training on data privacy responsibilities and best practices.

These measures align with applicable privacy standards and protect against unauthorized disclosure or misuse.

Secure System Maintenance

Explore performs system maintenance in a controlled and secure manner to ensure updates do not disrupt security mechanisms.

Key practices include:

- **Defined Maintenance Windows**: Scheduled and communicated to stakeholders.
- **Change Management Procedures**: Includes risk assessment, approvals, and rollback planning.
- **Security Validation Post-Maintenance**: Automated and manual checks confirm security controls remain intact.
- **Segregation of Duties**: Authorized personnel perform tasks, with activity logging.
- **Monitoring and Alerting**: Real-time tools detect anomalies during and after maintenance.

These practices ensure maintenance supports system stability and security.

Patch Management

Explore follows a structured patch management process to protect the MCC system from emerging vulnerabilities.

Key elements include:

- **Scheduled Patching**: Conducted during defined maintenance windows.
- **Out-of-Band Patching**: Performed for critical vulnerabilities.
- **Validation and Testing**: Ensures compatibility and avoids unintended impacts.
- **Change Management Oversight**: Includes documentation and rollback planning.
- **Monitoring and Reporting**: Tracks patch status and system stability.

This approach ensures timely remediation and operational continuity.

Locked-Down System Deployment

Explore supports deployment of the MCC system in a locked-down configuration to reduce vulnerabilities and minimize the attack surface.

Capabilities include:

- **Configurable Installation Options**: Only necessary components are enabled.

Internal

- **OS Hardening**: Disables unnecessary services and protocols.
- **User Account Restrictions**: Only required accounts are created; all others are disabled. Accounts are configured following the principle of least privilege, ensuring users and services have only the minimum access necessary to perform their functions.
- **Security Baseline Alignment**: Follows NIST and CIS hardening guidelines.
- **Change Control and Audit Logging**: Tracks configuration changes for monitoring and review.

This ensures secure deployment with minimal exposure.

Incident Management

Explore has a formal incident management procedure for suspected or confirmed intrusions.

Process includes:

- **Detection and Alerting**: Real-time monitoring and EDR alerts.
- **Initial Triage and Investigation**: SOC team assesses severity.
- **Internal Escalation**: Involves stakeholders based on severity.
- **Jurisdiction Notification**: Prompt notification per contractual obligations.
- **Containment and Remediation**: Isolates systems and applies fixes.
- **Post-Incident Review**: Documents findings and recommendations.

This ensures timely, transparent, and accountable incident response.

Data Integrity and System Assurance

Explore ensures data integrity through:

- **Transactional Integrity Controls**: ACID-compliant database operations.
- **Validation Rules**: Prevent incorrect or malformed data.
- **Audit Logging**: Tracks data changes for traceability.
- **Encryption and Secure Transmission**: Prevents tampering during transit and storage.

System assurance is supported by:

- SOC 2 Type 2-compliant infrastructure
- Automated monitoring and failover mechanisms
- Formal change management processes

These capabilities ensure reliable and secure operations.

Database Synchronization

If multiple databases are used, Explore ensures consistency through:

- **Real-Time Replication**: Secure synchronization protocols.
- **Consistency Checks**: Scheduled integrity and reconciliation processes.
- **Event-Driven Updates**: Controlled propagation of changes.
- **Monitoring and Alerting**: Detects delays or failures.

These procedures maintain data accuracy and availability across the system.

Internal

Security Certification and Accreditation

Explore provides documentation through the **IT Security Certification workbook** and maintains updated records in our GRC system.
Please refer to the attached completed Section 07-09-IT_Security_Certification_EXPLORE.xlxs Excel workbook provided by OCC as part of this RFP submission.

Security Testing

Explore Information Services employs a comprehensive and multi-layered approach to security testing for the MCC IRP/IFTA system, designed to ensure that both the application and its hosting environment remain resilient against evolving cybersecurity threats. Explore has robust security protocols and continues to enhance these measures through ongoing support, maintenance, and validation activities.

Security testing is conducted by a dedicated internal Security Team and supplemented by third-party experts to ensure independent verification and alignment with industry standards. This hybrid model provides continuous oversight and strengthens the overall security posture of the MCC system.

Penetration Testing and Vulnerability Assessment

Explore conducts annual penetration testing to simulate real-world attack scenarios and validate system resilience. These tests include manual assessments of critical areas such as:

- Non-repudiation
- Access control
- Session management
- Information leakage
- Audit and logging mechanisms
- Input validation

In addition to manual testing, automated vulnerability scanning tools are deployed across the infrastructure to detect known vulnerabilities. These scans are reviewed weekly by IT administrators and formally assessed during monthly vulnerability review sessions.

Explore also performs Static and Dynamic Application Security Testing (SAST/DAST) using tools such as Invicti, Tenable, Contrast Security, and GitHub with security features enabled. These tools simulate attacks and evaluate application vulnerabilities during both development and post-deployment phases.

Secure Development Practices

Security is embedded into Explore's software development lifecycle through:

- **Secure Code Reviews**: Conducted during development cycles to ensure adherence to secure coding standards and prevent the introduction of security flaws.

Internal

- **Testing Methodology**: Explore's methodology is based on recognized frameworks such as the OWASP Testing Guide and the Open-Source Security Testing Methodology Manual (OSSTMM). It includes the following phases:
    - Information Gathering
    - Planning and Analysis
    - Vulnerability Detection
    - Penetration Testing
    - Reporting and Remediation

This structured approach ensures that vulnerabilities are identified early and addressed promptly, maintaining a strong security posture throughout the system lifecycle.

Defense-in-Depth Strategy

Explore ensures the security and confidentiality of State Data collected through the MCC IRP/IFTA system by implementing a defense-in-depth strategy that spans technical, procedural, and organizational layers. Key provisions include:

- **Layered Security Controls**:
    - Physical security of hosting environments
    - Network-level protections (e.g., firewalls, intrusion detection systems)
    - Operating system hardening
    - Application-level safeguards (e.g., access control, encryption, secure coding)
- **Encryption of Data**: All State Data is encrypted both in transit (HTTPS/TLS) and at rest (industry-standard algorithms).
- **Access Management**: RBAC and jurisdiction-specific permissions ensure that only authorized users access sensitive data. MFA is available and can be enabled upon jurisdiction request.
- **24/7 Security Monitoring**: A dedicated security team monitors system activity continuously using advanced tools and analytics, enabling early detection and rapid response to threats.

Documentation and Transparency

Explore is committed to transparency and collaboration with the State of Oklahoma regarding the security posture of the MCC IRP/IFTA system. As part of this commitment, Explore will provide the following documentation:

- **Executive Summary of the Annual Penetration Test Report**: Includes scope, methodology, key findings, and remediation actions. Testing is performed by qualified professionals using OWASP and OSSTMM methodologies.

Additional documentation may be provided upon request and subject to confidentiality agreements, including:

- SOC 2 Type 2 Audit Summary

Internal

- Summary-level Vulnerability Scan Reports
- Security Incident Response Procedures
- Change Management and Patch Management Policies

These documents demonstrate Explore's proactive approach to security validation and alignment with best practices and compliance standards.

Internal and External Validation

Explore employs a hybrid security testing model that combines internal expertise with external validation:

- **Internal Security Team**: Conducts regular assessments including vulnerability scanning, secure code reviews, and configuration audits using OWASP and OSSTMM methodologies.
- **Third-Party Penetration Testing**: Engages specialized external firms to perform independent testing of the MCC application and infrastructure, providing objective evaluations and validating internal findings.

This combination ensures comprehensive coverage and continuous improvement of the MCC system's security posture.

Internal

Section Seven: Explore Development Approach

Development Methodology

Explore Information Services applies a structured, Agile-based development methodology to deliver the MCC IRP/IFTA system. This approach emphasizes adaptability, transparency, and continuous stakeholder engagement, ensuring the solution evolves in alignment with jurisdictional priorities and operational needs.

The MCC IRP/IFTA project follows a clearly defined lifecycle, with each phase contributing to the successful delivery and adoption of the system:

- **Project Initiation**
  Establishes governance, communication protocols, and project infrastructure. Key stakeholders are identified, and initial planning artifacts are created.

- **Project Planning**
  Refines the implementation strategy based on the RFP and Explore's experience with similar projects. A key activity during this phase is the Fit-Gap Assessment, which evaluates the alignment between the proposed solution and jurisdiction-specific requirements, dependencies, and constraints. This collaborative process helps identify potential gaps early, allowing for thoughtful adjustments to the project schedule and scope. While the initial schedule is based on RFP requirements, the Fit-Gap Assessment ensures it reflects real-world conditions and jurisdictional priorities, enhancing transparency and predictability.

- **Development Phase**
  The project scope is divided into distinct milestones, each delivering a functional component of the system. These milestones follow a structured lifecycle (detailed below), allowing for incremental delivery, early validation, and continuous feedback.

- **User Acceptance Testing (UAT)**
  Conducted after all milestones have been delivered, UAT provides jurisdictions with the opportunity to validate the complete system in a controlled environment prior to implementation.

- **Implementation**
  Includes final deployment activities, data migration, training, and transition to production. Explore works closely with jurisdictions to ensure a smooth and coordinated rollout.

- **Post-Implementation/Warranty Support**
  Provides ongoing support to address any post-launch issues, ensure system stability, and assist with user adoption.

Internal

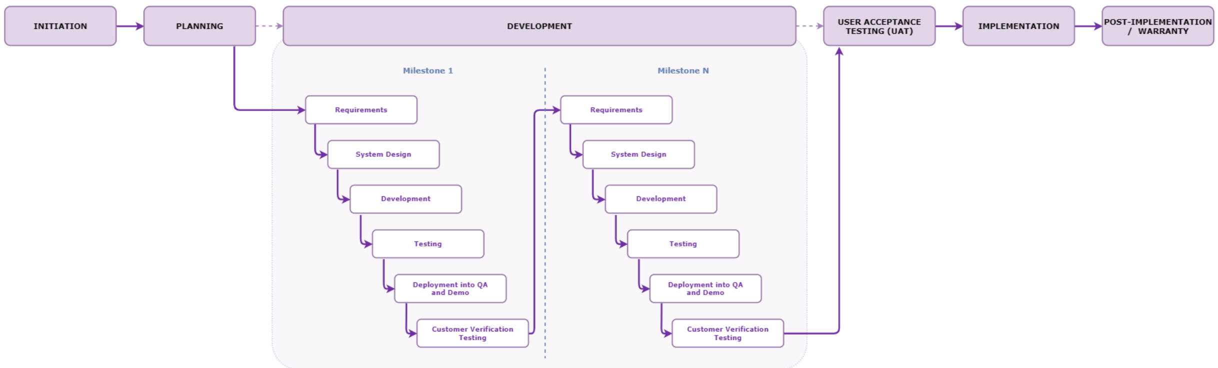


Figure 1 MCC Project Lifecycle

Benefits of Iterative Delivery

Explore's Agile methodology offers several key advantages:

- **Flexibility**: Requirements can be refined as the project progresses, allowing the system to adapt to changing needs or priorities.
- **Early Feedback**: Stakeholders are engaged throughout development, enabling timely input and reducing the risk of misalignment.
- **Reduced Risk**: By delivering functionality in stages, Explore can identify and address issues early, minimizing the impact of defects or scope changes.
- **Improved Quality**: Continuous integration and testing ensure that each increment meets quality standards before moving forward.

This approach aligns with industry-recognized best practices, including those outlined by the Project Management Institute (PMI), and supports a delivery model that is both structured and responsive.

Tools and Frameworks

Explore leverages a suite of modern tools and frameworks to support Agile development and DevOps practices:

- **Microsoft Project**: Facilitates overall project planning, scheduling, and progress tracking
- **Jira**: Used for work item planning, tracking, and lifecycle management across milestones
- **GitHub**: Provides secure version control, code review workflows, and integrated security scanning
- **TestRail**: Supports structured QA processes, test case management, and traceability
- **DevOps Pipelines**: Automated build, test, and deployment pipelines ensure consistent delivery and reduce manual errors

Together, these tools enable Explore to deliver a robust, scalable MCC IRP/IFTA system with precision, agility and accountability.

Internal

Project Milestones and Deliverables

Explore Information Services structures the MCC IRP/IFTA system implementation around a series of iterative milestones, each representing a complete cycle of development activities. This approach supports flexibility, continuous feedback, and incremental delivery of working functionality, rather than a traditional waterfall model.

Each milestone within the Development Phase follows a repeatable lifecycle designed to promote quality, transparency, and stakeholder engagement.

Requirements Gathering → System Design → Development → Testing → Deployment into QA Environment and Demo → Customer Verification Testing

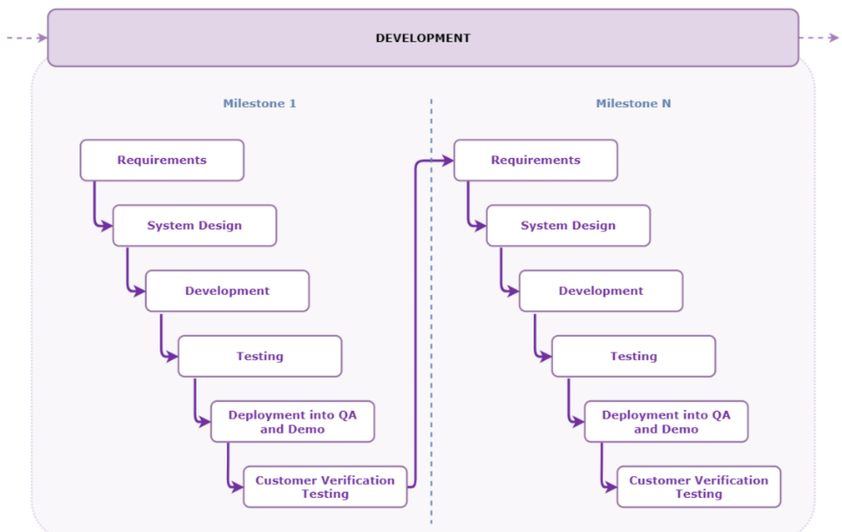


Figure 2 Milestone Lifecycle

This structure enables Explore to deliver functional components incrementally, allowing jurisdictions to review and validate features as they are developed. Customer Verification Testing is conducted throughout the development phase, providing early insight into system capabilities and reducing the risk of misalignment. This process is distinct from the formal UAT, which occurs at the end of the project.

Explore's development process consists of the following steps:

- **Requirements Gathering**: Conducted collaboratively with Oklahoma stakeholders, this phase focuses on defining business needs and jurisdiction-specific requirements for each milestone. Explore facilitates Joint Application Design (JAD) sessions, which serve not only as a forum for requirement elicitation but also as an opportunity to educate stakeholders on the functionality and capabilities of the module being developed. These sessions are interactive, allowing stakeholders to gain a deeper understanding of how the system will support their operations. Explore's team provides hands-on walkthroughs, demonstrations,

Internal

and contextual training during these sessions to ensure that stakeholders are well-informed and able to contribute meaningfully to the design process.

- **System Design:** Focused on the technical architecture for custom interfaces required by Oklahoma, including integration points with external systems, data exchanges, and jurisdictional workflows.
- **Development:** Coding and configuration of features defined for the milestone, including unit testing and integration of components.
- **Testing:** Execution of system testing by Explore's System Quality Assurance (SQA) team to validate milestone-specific functionality and ensure readiness for stakeholder review.
- **Deployment into QA Environment**: Explore continuously deploys completed functionality into a customer-accessible QA environment, allowing stakeholders to interact with the system as it evolves. This early access supports hands-on familiarity, accelerates issue identification, and simplifies future activities such as UAT and training. By experiencing the system in real time, stakeholders gain confidence in its capabilities and contribute valuable feedback throughout development. *(Refer to MCC Environments Diagram)*.
- **Verification Testing:** Conducted by OCC staff in the QA environment to perform high-level validation of delivered functionality. This testing confirms that the milestone meets jurisdictional expectations and is ready for approval.

This iterative structure allows Explore to deliver value early and often, while maintaining alignment with Oklahoma's evolving needs.

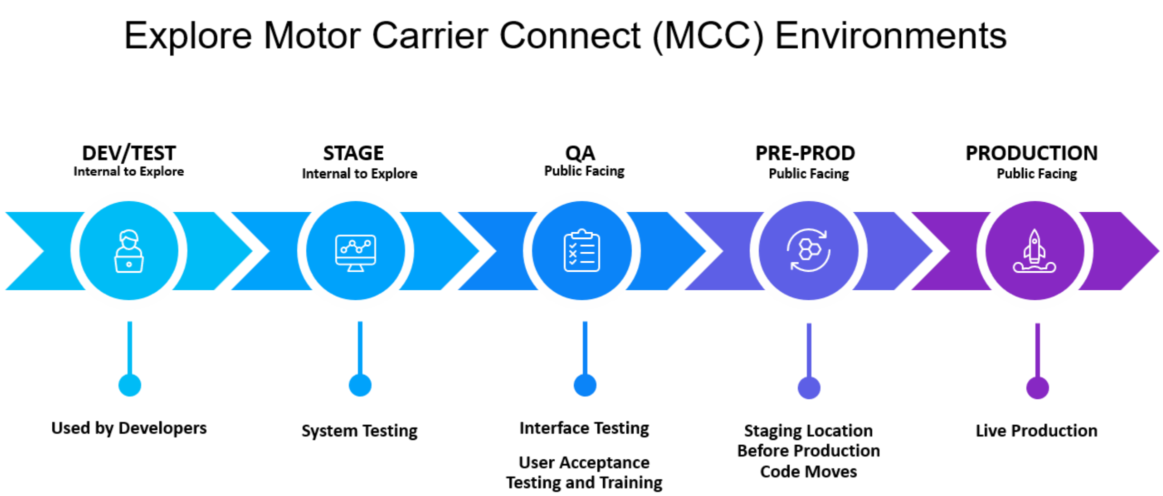


Figure 3 Explore MCC Environments

Project Schedule and Timeline

Explore has provided a detailed draft project schedule and sample milestone matrix to support planning and execution. These documents outline:

- Iteration timelines and expected delivery dates

Internal

- Scope of functionality for each milestone
- Key dependencies and resource planning considerations
- Alignment with billing events and payment terms

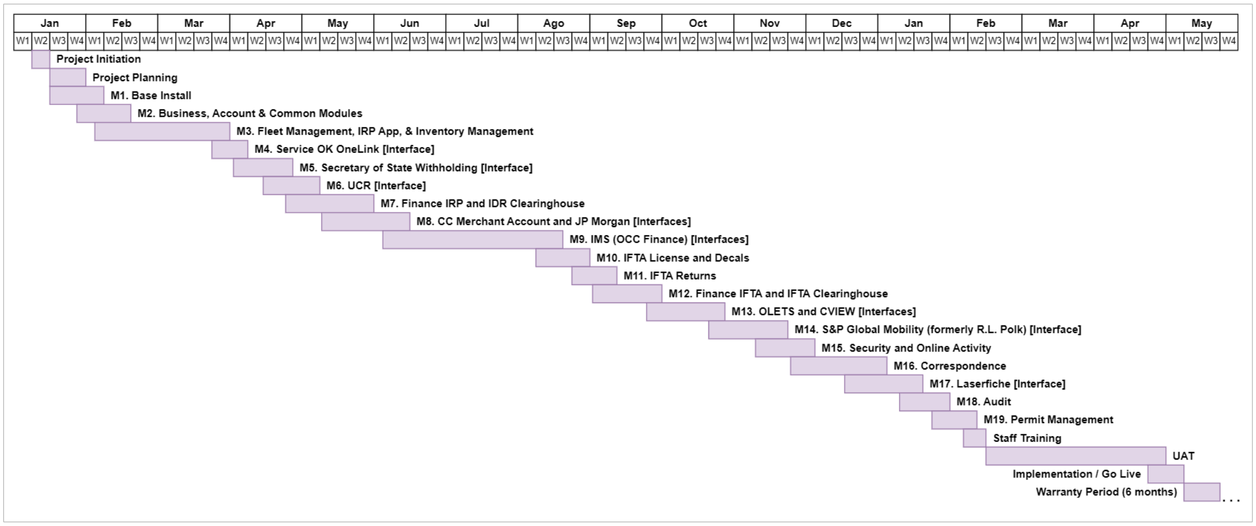


Figure 4 Draft Project Gantt Chart

As this schedule is preliminary, it will be refined during project initiation through collaborative planning and the fit-gap assessment. Adjustments will be made based on priority, risk, and stakeholder input. Milestones may also be merged or restructured where appropriate to streamline delivery and optimize resource utilization.

Table 1 Draft OCC IRP, IFTA, Permit Schedule

WBS	Task Name	Duration	Start	Finish
1	**OK IRP & IFTA MCC Project**	**442.91 days**	**Tue 1/6/26**	**Thu 5/6/27**
1.1	**Project Initiation**	**6.46 days**	**Tue 1/6/26**	**Tue 1/13/26**
1.1.1	Set up Project Tools	5.13 days	Tue 1/6/26	Mon 1/12/26
1.1.2	Kickoff Meeting	2 hrs	Tue 1/13/26	Tue 1/13/26
1.1.3	*Milestone Accepted/Completed - Project Kick-off Meeting*	*0 days*	*Tue 1/13/26*	*Tue 1/13/26*
1.2	**Project Planning**	**13 days**	**Tue 1/13/26**	**Wed 1/28/26**
1.2.1	Project Documentation	7.67 days	Tue 1/13/26	Thu 1/22/26
1.2.2	Customer Review and Approval	5.33 days	Thu 1/22/26	Wed 1/28/26
1.2.3	*Milestone Accepted/Completed - Project Planing*	*0 days*	*Wed 1/28/26*	*Wed 1/28/26*
1.3	**Milestone 1 - Base Install**	**23.5 days**	**Tue 1/13/26**	**Mon 2/9/26**
1.3.1	Base Installation (Set up new DB in all environments, URL, site header, state logo and seal for forms)	8.33 days	Tue 1/13/26	Thu 1/22/26
1.3.2	Base Configuration (Worksheets)	7.67 days	Thu 1/15/26	Mon 1/26/26
1.3.3	Security Intro / overview (BA time only)	4 hrs	Tue 1/20/26	Tue 1/20/26
1.3.4	Customer Testing and Acceptance	13.33 days	Mon 1/26/26	Mon 2/9/26

Internal

WBS	Task Name	Duration	Start	Finish
1.3.5	*Milestone Accepted/Completed - Milestone 1 - Base Install*	*0 days*	*Mon 2/9/26*	*Mon 2/9/26*
1.4	**Milestone 2 - Business, Account and Common Modules**	**20.55 days**	**Mon 1/26/26**	**Tue 2/17/26**
1.4.1	Business Management	2.75 days	Mon 1/26/26	Wed 1/28/26
1.4.2	Account Management	3.82 days	Tue 1/27/26	Fri 1/30/26
1.4.3	Common Modules	4.67 days	Wed 1/28/26	Tue 2/3/26
1.4.4	Customer Testing and Acceptance	13.33 days	Tue 2/3/26	Tue 2/17/26
1.4.5	*Milestone Accepted - Milestone 2 - Business, Account and Common Modules*	*0 days*	*Tue 2/17/26*	*Tue 2/17/26*
1.5	**Milestone 3 - Fleet Management, IRP Applications and Inventory Management, and PRISM interface**	**54.4 days**	**Wed 2/4/26**	**Wed 4/1/26**
1.5.1	Fleet Management	10.42 days	Wed 2/4/26	Fri 2/13/26
1.5.2	Jurisdiction, Weight Groups and Units Management	20 days	Mon 2/9/26	Mon 3/2/26
1.5.3	Base Jurisdiction Fee Calculation	17.58 days	Mon 2/16/26	Fri 3/6/26
1.5.4	IRP Required Documents	12.58 days	Fri 2/20/26	Thu 3/5/26
1.5.5	Inventory Management	13.92 days	Tue 2/24/26	Tue 3/10/26
1.5.6	Apps Sub-Functions	11.17 days	Mon 3/2/26	Thu 3/12/26
1.5.7	IRP Application Processing	14.08 days	Tue 3/3/26	Wed 3/18/26
1.5.8	Performance Registration Information Systems Management (PRISM) [Interface]	12.08 days	Thu 3/5/26	Wed 3/18/26
1.5.9	Customer Testing and Acceptance	13.23 days	Wed 3/18/26	Wed 4/1/26
1.5.10	*Milestone Accepted - Milestone 3 - Fleet Management, IRP Applications and Inventory Management*	*0 days*	*Wed 4/1/26*	*Wed 4/1/26*
1.6	**Milestone 4 - Service OK OneLink [Interface]**	**17.83 days**	**Mon 3/23/26**	**Thu 4/9/26**
1.6.1	Service OK OneLink [Interface]	5.83 days	Mon 3/23/26	Fri 3/27/26
1.6.2	Customer Testing and Acceptance	12 days	Fri 3/27/26	Thu 4/9/26
1.6.3	*Milestone Accepted - Milestone 4 - Service OK OneLink [Interface]*	*0 days*	*Thu 4/9/26*	*Thu 4/9/26*
1.7	**Milestone 5 - Secretary of State Withholding [Interface]**	**17.83 days**	**Fri 4/3/26**	**Thu 4/23/26**
1.7.1	**Secretary of State Withholding [Interface]**	5.83 days	Fri 4/3/26	Fri 4/10/26
1.7.2	**Customer Testing and Acceptance**	12 days	Fri 4/10/26	Thu 4/23/26
1.7.3	*Milestone Accepted -Milestone 5 - Secretary of State Withholding [Interface]*	*0 days*	*Thu 4/23/26*	*Thu 4/23/26*
1.8	**Milestone 6 - UCR [Interface] (Potential)**	**19.17 days**	**Mon 4/13/26**	**Mon 5/4/26**
1.8.1	UCR [Interface]	6.5 days	Mon 4/13/26	Mon 4/20/26
1.8.2	Customer Testing and Acceptance	12.67 days	Mon 4/20/26	Mon 5/4/26
1.8.3	*Milestone Accepted - Milestone 7 - UCR [Interface] (Potential)*	*0 days*	*Mon 5/4/26*	*Mon 5/4/26*
1.9	**Milestone 7 - Finance IRP and IDR Clearinghouse**	**38.04 days**	**Tue 4/21/26**	**Mon 6/1/26**
1.9.1	Finance Management (IRP)	17.04 days	Tue 4/21/26	Fri 5/8/26
1.9.2	IDR Clearinghouse [Interface]	9.04 days	Wed 4/29/26	Fri 5/8/26
1.9.3	Customer Testing and Acceptance	20.33 days	Fri 5/8/26	Mon 6/1/26
1.9.4	*Milestone Accepted - Milestone 8 - Finance IRP*	*0 days*	*Mon 6/1/26*	*Mon 6/1/26*
1.1	**Milestone 8 - CC Merchant Account and JP Morgan [Interfaces]**	**29.25 days**	**Mon 5/11/26**	**Thu 6/11/26**
1.10.1	CC Merchant Account [Interface]	11.42 days	Mon 5/11/26	Fri 5/22/26

Internal

WBS	Task Name	Duration	Start	Finish
1.10.2	JP Morgan [Interface]	14.58 days	Thu 5/14/26	Mon 6/1/26
1.10.3	Customer Testing and Acceptance	11.33 days	Mon 6/1/26	Thu 6/11/26
1.10.4	*Milestone Accepted - Milestone 9 - CC Merchant Account [Interface]*	*0 days*	*Thu 6/11/26*	*Thu 6/11/26*
1.11	**Milestone 9 - IMS (OCC Finance) [Interface]**	**74 days**	**Tue 6/2/26**	**Thu 8/20/26**
1.11.1	IMS (OCC Finance) [Interface]	60.33 days	Tue 6/2/26	Thu 8/6/26
1.11.2	Customer Testing and Acceptance	13.67 days	Thu 8/6/26	Thu 8/20/26
1.11.3	*Milestone Accepted - Milestone 11 - IMS (OCC Finance) [Interface]*	*0 days*	*Thu 8/20/26*	*Thu 8/20/26*
1.12	**Milestone 10 - IFTA License and Decals**	**23.33 days**	**Fri 8/7/26**	**Tue 9/1/26**
1.12.1	IFTA License and Decals Management	8 days	Fri 8/7/26	Mon 8/17/26
1.12.2	Inventory Management	5 days	Thu 8/13/26	Tue 8/18/26
1.12.3	Customer Testing and Acceptance	13.33 days	Tue 8/18/26	Tue 9/1/26
1.12.4	*Milestone Accepted - Milestone 13 - IFTA License and Decals*	*0 days*	*Tue 9/1/26*	*Tue 9/1/26*
1.13	**Milestone 11 - IFTA Returns**	**21.17 days**	**Wed 8/19/26**	**Fri 9/11/26**
1.13.1	IFTA Returns Management	7.83 days	Wed 8/19/26	Thu 8/27/26
1.13.2	Customer Testing and Acceptance	13.33 days	Thu 8/27/26	Fri 9/11/26
1.13.3	*Milestone Accepted - Milestone 14 - IFTA Returns*	*0 days*	*Fri 9/11/26*	*Fri 9/11/26*
1.14	**Milestone 12 - Finance IFTA and IFTA Clearinghouse**	**30.04 days**	**Fri 8/28/26**	**Wed 9/30/26**
1.14.1	Finance Management (IFTA)	9.71 days	Fri 8/28/26	Wed 9/9/26
1.14.2	IFTA Clearinghouse [Interface]	6.38 days	Thu 9/3/26	Thu 9/10/26
1.14.3	Customer Testing and Acceptance	20.33 days	Wed 9/9/26	Wed 9/30/26
1.14.4	*Milestone Accepted - Milestone 15 - Finance IFTA*	*0 days*	*Wed 9/30/26*	*Wed 9/30/26*
1.15	**Milestone 13 - OLETS and CVIEW [Interfaces]**	**29.67 days**	**Fri 9/25/26**	**Tue 10/27/26**
1.15.1	OLETS [Interface]	17.33 days	Fri 9/25/26	Wed 10/14/26
1.15.2	CVIEW [Interface]	14.5 days	Wed 9/30/26	Thu 10/15/26
1.15.3	Customer Testing and Acceptance	12.33 days	Wed 10/14/26	Tue 10/27/26
1.15.4	*Milestone Accepted - Milestone 17 - OLETS [Interface]*	*0 days*	*Tue 10/27/26*	*Tue 10/27/26*
1.16	**Milestone 14 - S&P Global Mobility (formerly R.L. Polk) [Interface]**	**28.83 days**	**Wed 10/21/26**	**Fri 11/20/26**
1.16.1	S&P Global Mobility (formerly R.L. Polk) [Interface]	16.5 days	Wed 10/21/26	Fri 11/6/26
1.16.2	Customer Testing and Acceptance	12.33 days	Fri 11/6/26	Fri 11/20/26
1.16.3	*Milestone Accepted -Milestone 19 - S&P Global Mobility (formerly R.L. Plk) [Interface]*	*0 days*	*Fri 11/20/26*	*Fri 11/20/26*
1.17	**Milestone 15 - Security and Online Activity**	**24.33 days**	**Mon 11/9/26**	**Mon 12/7/26**
1.17.1	Security Management	7.67 days	Mon 11/9/26	Tue 11/17/26
1.17.2	Online Activity	4.67 days	Mon 11/16/26	Fri 11/20/26
1.17.3	Reports Management	3 days	Wed 11/18/26	Fri 11/20/26
1.17.4	Core Interface	2.67 days	Thu 11/19/26	Mon 11/23/26
1.17.5	Iteration [9] Code Move	0.67 days	Mon 11/23/26	Tue 11/24/26
1.17.6	Demo and Customer Testing	10.33 days	Tue 11/24/26	Mon 12/7/26
1.17.7	*Milestone Accepted - Milestone 20 - Security and Online Activity*	*0 days*	*Mon 12/7/26*	*Mon 12/7/26*
1.18	**Milestone 16 - Correspondence (SMS, Document Management, Account Correspondence, Mass Communication)**	**32 days**	**Mon 11/23/26**	**Thu 1/7/27**

WBS	Task Name	Duration	Start	Finish
1.18.1	Correspondence	19.67 days	Mon 11/23/26	Wed 12/16/26
1.18.2	Customer Testing and Acceptance	12.33 days	Wed 12/16/26	Thu 1/7/27
1.18.3	*Milestone Accepted - Milestone 21 - Correspondence (SMS, Document Management, Account Correspondence, Mass Communication)*	*0 days*	*Thu 1/7/27*	*Thu 1/7/27*
1.19	**Milestone 17 - Laserfiche [Interface]**	**23.67 days**	**Thu 12/17/26**	**Fri 1/22/27**
1.19.1	Laserfiche [Interface]	11.33 days	Thu 12/17/26	Thu 1/7/27
1.19.2	Customer Testing and Acceptance	12.33 days	Thu 1/7/27	Fri 1/22/27
1.19.3	*Milestone Accepted - Milestone 22 - Laserfiche [Interface]*	*0 days*	*Fri 1/22/27*	*Fri 1/22/27*
1.2	**Milestone 18 - Audit**	**19 days**	**Fri 1/8/27**	**Fri 1/29/27**
1.20.1	IFTA Audit Management	4.67 days	Fri 1/8/27	Thu 1/14/27
1.20.2	IRP Audit Management	4.33 days	Wed 1/13/27	Tue 1/19/27
1.20.3	Audit Correspondence	2 days	Fri 1/15/27	Wed 1/20/27
1.20.4	Customer Testing and Acceptance	10.33 days	Wed 1/20/27	Fri 1/29/27
1.20.5	*Milestone Accepted - Milestone 23 - Audit*	*0 days*	*Fri 1/29/27*	*Fri 1/29/27*
1.21	**Milestone 19 - Permits Management (Trip, Fuel, Bulk Permits)**	**23 days**	**Wed 1/20/27**	**Mon 2/15/27**
1.21.1	Permits Management (Trip, Fuel, Bulk Permits)	10.67 days	Wed 1/20/27	Mon 2/1/27
1.21.2	Customer Testing and Acceptance	12.33 days	Mon 2/1/27	Mon 2/15/27
1.21.3	*Milestone Accepted - Milestone 25 - Permits Management (Trip, Fuel, Bulk Permits)*	*0 days*	*Mon 2/15/27*	*Mon 2/15/27*
1.22	**Data Conversion**	**412.95 days?**	**Mon 2/9/26**	**Thu 5/6/27**
1.22.1	Jurisdiction Data Security Process	0 days	Mon 2/9/26	Mon 2/9/26
1.22.2	Converting Data (~4 months)	116 days	Fri 2/13/26	Wed 6/17/26
1.22.3	Production Data Loads (from legacy system)	406.45 days?	Fri 2/13/26	Thu 5/6/27
1.22.4	*Milestone Accepted/Completed - Data Conversion*	*0 days*	*Thu 5/6/27*	*Thu 5/6/27*
1.23	**User Manuals Updates**	**365.41 days**	**Tue 1/6/26**	**Mon 2/15/27**
1.23.1	User Manuals Updates	200 days	Tue 1/6/26	Mon 8/10/26
1.23.2	*Milestone Accepted/Completed - User Manuals Updates*	*0 days*	*Mon 2/15/27*	*Mon 2/15/27*
1.24	**Staff Training**	**4 days**	**Wed 2/10/27**	**Mon 2/15/27**
1.24.1	Training	4 days	Wed 2/10/27	Mon 2/15/27
1.24.2	*Milestone Accepted/Completed - Staff Training*	*0 days*	*Mon 2/15/27*	*Mon 2/15/27*
1.25	**User Acceptance Testing (UAT)**	**70.5 days**	**Mon 2/15/27**	**Thu 4/29/27**
1.25.1	Testing Hold	0.5 days	Mon 2/15/27	Tue 2/16/27
1.25.2	*Start of UAT*	*0 days*	*Tue 2/16/27*	*Tue 2/16/27*
1.25.3	Customer UAT	70 days	Tue 2/16/27	Thu 4/29/27
1.25.4	Certification process (IFTA CH, IRP CH, CVIEW)	15 days	Wed 4/14/27	Thu 4/29/27
1.26	**Implementation / Go Live Week**	**9 days**	**Tue 4/27/27**	**Thu 5/6/27**
1.26.1	Go Live Activities	**9 days**	Tue 4/27/27	Thu 5/6/27
1.26.2	*Milestone Accepted/Completed - Implementation*	*0 days*	*Thu 5/6/27*	*Thu 5/6/27*
2	**Warranty Period**	**170**	**Thu 5/6/27**	**Thu 11/5/27**
2.1	Warranty Period	169	Thu 5/6/27	Thu 11/4/27
2.2	*End of the Warranty Period*	*1 day*	*Thu 11/4/27*	*Thu 11/5/27*

Internal

Milestone Matrix

The Milestone Matrix table provides a comprehensive overview of all project milestones planned throughout the implementation lifecycle. Each milestone represents a key delivery point tied to specific functionality, activities, or project phases. The table includes a column labeled "Billable Milestone", which identifies the milestones that are eligible for invoicing upon successful completion. Milestone completion will be tied to billing events, with payment amounts and terms to be finalized during contract negotiations. This structure ensures transparency in billing and aligns payment events with tangible progress, allowing the Oklahoma Corporation Commission to track deliverables and associated costs with clarity.

Table 2 Draft Milestone Matrix

1	OK IRP & IFTA MCC Project	Billable Milestone	Planned Completion Date
1.1	Project Initiation	No	Tue 1/13/26
1.2	Project Planning	No	Wed 1/28/26
1.3	Milestone 1 - Base Install	Yes	Mon 2/9/26
1.4	Milestone 2 - Business, Account and Common Modules	No	Tue 2/17/26
1.5	Milestone 3 - Fleet Management, IRP Applications and Inventory Management, and PRISM interface	Yes	Wed 4/1/26
1.6	Milestone 4 - Service OK OneLink [Interface]	Yes	Thu 4/9/26
1.7	Milestone 5 - Secretary of State Withholding [Interface]	Yes	Thu 4/23/26
1.8	Milestone 6 - UCR [Interface] (Potential)	Yes	Mon 5/4/26
1.9	Milestone 7 - Finance IRP and IDR Clearinghouse	No	Mon 6/1/26
1.1	Milestone 8 - CC Merchant Account and JP Morgan [Interfaces]	Yes	Thu 6/11/26
1.11	Milestone 9 - IMS (OCC Finance) [Interface]	Yes	Thu 8/20/26
1.12	Milestone 10 - IFTA License and Decals	No	Tue 9/1/26
1.13	Milestone 11 - IFTA Returns	Yes	Fri 9/11/26
1.14	Milestone 12 - Finance IFTA and IFTA Clearinghouse	No	Wed 9/30/26
1.15	Milestone 13 - OLETS and CVIEW [Interfaces]	Yes	Tue 10/27/26
1.16	Milestone 14 - S&P Global Mobility (formerly R.L. Polk) [Interface]	Yes	Fri 11/20/26
1.17	Milestone 15 - Security and Online Activity	No	Mon 12/7/26
1.18	Milestone 16 - Correspondence (SMS, Document Management, Account Correspondence, Mass Communication)	Yes	Thu 1/7/27
1.19	Milestone 17 - Laserfiche [Interface]	Yes	Fri 1/22/27
1.2	Milestone 18 - Audit	No	Fri 1/29/27
1.21	Milestone 19 - Permits Management (Trip, Fuel, Bulk Permits)	Yes	Mon 2/15/27
1.22	Data Conversion (Completion)	Yes	Wed 6/17/26
1.23	User Manuals Updates	No	Mon 2/15/27
1.24	Staff Training	Yes	Mon 2/15/27
1.25	User Acceptance Testing (UAT) - Start Date	Yes	Mon 2/15/27
1.26	Implementation / Go Live Week	Yes	Thu 5/6/27
2	Warranty Period (6 months)	No	Thu 11/5/27

Milestone Completion and Approval Criteria

Each milestone will be subject to verification testing and stakeholder review to confirm that the delivered functionality meets the agreed-upon scope. This process includes:

- **Verification Testing**: Targeted testing of milestone-specific features by OCC in the QA environment. This testing validates correctness and readiness but is not full UAT.
- **Documentation Review**: Confirmation that required technical and functional documentation has been delivered and approved.
- **Stakeholder Sign-Off**: Formal approval from designated State representatives confirming that the milestone has been satisfactorily completed.

Deployment

For this project, deployment into the Production environment will occur only after all milestone development activities have been completed, the data conversion process has been finalized and successfully tested, and User Acceptance Testing (UAT) has been completed and approved by the State.

Explore will not proceed with implementation until these critical prerequisites are met, ensuring that the MCC IRP/IFTA system is fully functional, jurisdictionally validated, and ready for live operations. This approach minimizes risk and ensures a smooth transition to production.

Once approved, Explore will coordinate closely with the Oklahoma Corporation Commission (OCC) to execute the production deployment, provide go-live support, and monitor system performance to ensure stability and responsiveness.

Verification Testing for Milestone Acceptance

Explore Information Services incorporates milestone-level verification testing as a critical step in the iterative development process for the MCC IRP/IFTA system. This testing is conducted by the Oklahoma Corporation Commission (OCC) in the Quality Assurance (QA) environment and serves as a formal checkpoint to validate that the functionality delivered in each milestone meets jurisdictional expectations before proceeding to full User Acceptance Testing (UAT) or production deployment.

Purpose and Scope

Verification testing is designed to:

- Confirm that the features and enhancements delivered in a given milestone are functioning as intended
- Validate that jurisdiction-specific requirements have been implemented correctly
- Identify any issues or gaps early in the development cycle, allowing for timely remediation

This testing is not intended to replace full UAT, but rather to provide a focused, high-level review of milestone-specific functionality. It ensures that each iteration is on track and that cumulative development aligns with the overall system goals.

Internal

Stakeholder Involvement

OCC staff play a central role in verification testing by:

- Reviewing the deployed functionality in the QA environment
- Providing feedback on usability, accuracy, and jurisdictional alignment
- Participating in milestone review sessions to discuss findings and confirm acceptance

Explore supports this process by preparing test environments, providing documentation, and addressing any issues identified during verification. Once OCC confirms that the milestone meets expectations, formal stakeholder sign-off is recorded, allowing the project to proceed to the next iteration. If the milestone is designated as billable, Explore will submit an invoice to OCC for the agreed-upon amount associated with that milestone.

This structured approach to verification testing ensures transparency, quality control, and collaborative validation throughout the development lifecycle.

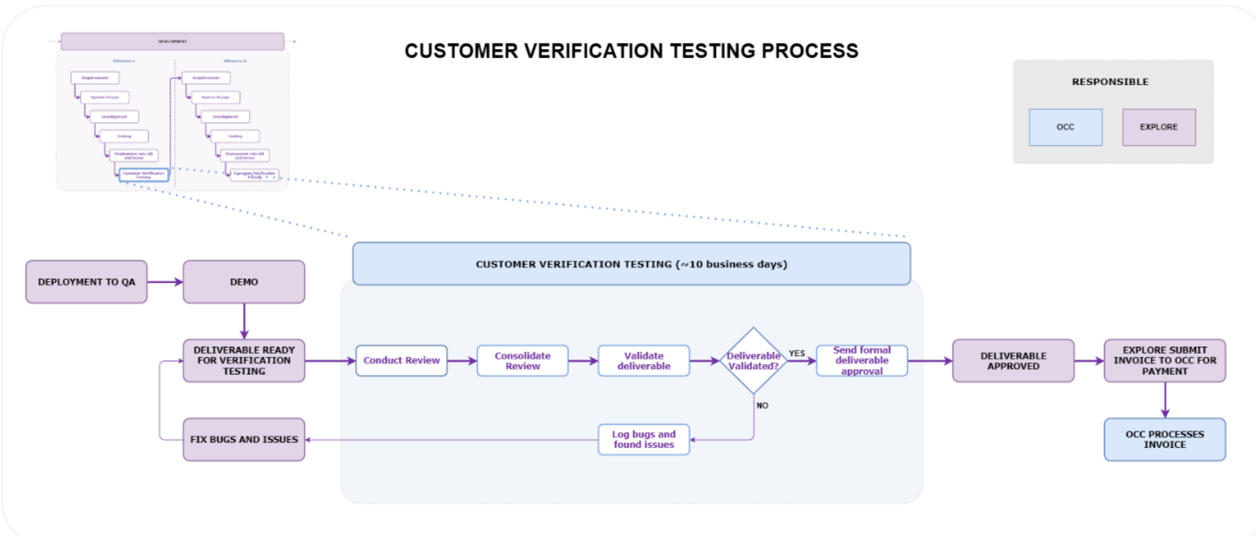


Figure 5 Customer Verification Testing Process

Types of Testing

Explore Information Services employs a comprehensive testing strategy to ensure the MCC IRP/IFTA system meets functional, technical, and security requirements throughout the development lifecycle. Testing is conducted across multiple layers and phases, with each type serving a distinct purpose in validating system quality and readiness.

Unit Testing

Unit testing is performed by Explore's development team during the coding phase. This testing focuses on individual components or modules of the system to ensure they function correctly in isolation. Unit tests are automated where possible and are executed continuously as part of the development pipeline to catch defects early.

Internal

System Testing

System testing is conducted by Explore's System Quality Assurance (SQA) team and involves end-to-end validation of integrated features. This testing ensures that all components work together as expected and that the system meets functional requirements. It includes testing of workflows, data exchanges, user interfaces, and jurisdiction-specific configurations.

Verification Testing

Verification testing is conducted by OCC staff in the QA environment to validate milestone-specific functionality prior to full UAT. This high-level testing confirms that the delivered features meet jurisdictional expectations and are ready for formal acceptance.

User Acceptance Testing (UAT)

UAT is led by the Oklahoma Corporation Commission (OCC) and other designated jurisdictional stakeholders. It is performed after all development and data conversion activities are complete and focuses on validating that the system meets business requirements and is ready for production use. Explore supports UAT by preparing test environments, providing test scripts, and resolving any issues identified during testing.

Regression Testing

Regression testing is conducted throughout the development lifecycle to ensure that new changes do not negatively impact existing functionality. This testing is automated where feasible and is executed during each milestone to maintain system stability and prevent reintroduction of previously resolved defects.

Security Testing

Explore performs security testing as part of its broader security validation program. This includes:

- **Penetration Testing**: Annual testing by internal or third-party experts to simulate real-world attack scenarios.
- **Vulnerability Scanning**: Continuous scanning using tools such as Tenable and Invicti to identify known vulnerabilities.
- **Secure Code Reviews and SAST/DAST**: Integrated into the development process to detect and remediate security flaws.

For more details, see Section 07-03 – Explore – Security and Data Protection.pdf document.

Performance Testing

Explore conducts performance testing prior to every production code release to ensure the MCC IRP/IFTA system meets expected performance benchmarks under load. This testing evaluates system responsiveness, stability, and scalability, and includes:

- Load testing to simulate concurrent user activity
- Stress testing to identify system limits
- Response time measurement for key transactions

- Resource utilization monitoring (CPU, memory, network)

Performance testing results are reviewed by the technical team and shared with stakeholders to confirm readiness for deployment.

Data Migration Strategy

Explore Information Services takes an iterative and collaborative approach to data migration for the MCC IRP/IFTA system. Rather than treating data conversion as a single, monolithic event, Explore integrates migration activities into the overall milestone/iteration flow. This strategy allows for early visibility of migrated data, faster feedback from stakeholders, and continuous refinement of mapping and transformation logic.

Iterative Migration Approach

Data migration begins early in the project and progresses in parallel with system development. Explore starts with foundational data domains such as business entities, accounts, addresses, and contacts, which are critical for system usability and stakeholder engagement.

For each iteration:

- Explore works with OCC to define the scope of data to be migrated
- Mapping logic is developed to align legacy data structures with MCC system formats
- Migration scripts are written and executed in the QA environment
- OCC staff begin reviewing and interacting with the migrated data

This approach allows OCC to see and use real data earlier, helping to identify gaps, inconsistencies, or jurisdiction-specific nuances that may not be evident during documentation review alone.

Data Mapping, Cleansing, and Validation

Explore performs detailed data mapping for each domain, ensuring that legacy values, codes, and formats are accurately translated into the MCC system. During each iteration:

- Data cleansing rules are applied to remove duplicates, correct formatting issues, and standardize entries
- Validation checks are performed to ensure completeness and accuracy
- Feedback from OCC is incorporated to refine mapping logic and improve data quality

As new data domains are added in subsequent iterations, Explore re-runs the data conversion process with all completed mappings and scripts to date. This ensures that the QA environment reflects the most current and complete data set available at each stage.

Testing and Reconciliation

While there is no formal verification testing or sign-off required for each data conversion iteration, Explore supports OCC in reviewing and validating the data through:

- Reconciliation reports comparing source and target data
- Spot checks and sample validations
- Issue tracking and resolution workflows

This informal but structured review process helps ensure that data quality improves with each iteration and that final migration is accurate and complete.

Jurisdiction Involvement

While there is no formal verification testing or sign-off required for each data conversion iteration, Explore supports OCC in reviewing and validating the data through:

- Reconciliation reports comparing source and target data
- Spot checks and sample validations
- Issue tracking and resolution workflows

To support this process, Explore will provide a high-level checklist and sample test cases to guide validation efforts. As data conversion progresses, Explore will document unique scenarios that warrant targeted testing and will encourage OCC to compile a list of accounts, data sets, and business scenarios for verification.

Explore also recommends parallel testing during UAT. As OCC staff enter transactions in their legacy production system, they should perform the same transactions on the corresponding accounts in the MCC QA environment to confirm expected results. This approach helps validate system behavior, uncover edge cases, and build confidence in the converted data and MCC functionality.

This informal but structured review process helps ensure that data quality improves with each iteration and that final migration is accurate and complete.

Implementation and Rollout

Explore Information Services follows a structured and collaborative approach to implementing the MCC IRP/IFTA system for the State of Oklahoma. Our strategy is designed to ensure a smooth and efficient transition from legacy systems to the new platform, with minimal disruption to operations and maximum stakeholder confidence.

Implementation Planning

Explore will develop a detailed Implementation Plan in coordination with the Oklahoma Corporation Commission (OCC). This plan will outline all activities required to prepare for go-live, including final data migration, system readiness checks, stakeholder communications, and contingency planning. The plan will be refined and updated collaboratively with OCC throughout the project lifecycle to ensure alignment with jurisdictional needs and expectations.

Cutover and Go-Live Strategy

Explore *typically* executes cutover and go-live activities over a single weekend to minimize operational downtime. The process includes:

- **Friday**: Final data migration and cutover from legacy systems

- **Saturday (and Sunday if needed)**: Acceptance testing by OCC staff in the production environment to validate readiness
- **Monday**: Full go-live for all users

To ensure a smooth transition, Explore assigns a dedicated staff member onsite during the cutover weekend and the first week of go-live. This individual provides hands-on support, facilitates communication between teams, and assists with issue resolution in real time.

End-User Training and Support

Explore provides comprehensive end-user training and support to ensure a successful transition. Training materials, sessions, and help desk support are tailored to the needs of OCC staff and jurisdictional users.
Note: Refer to Section 07-05 – Explore - Documentation and Training.pdf document.
Explore also offers post-training support through help desk services, knowledge base resources, and direct engagement with jurisdictional teams to address questions and ensure user confidence.

Post-Implementation Monitoring

Following production deployment, Explore initiates post-implementation monitoring to ensure system stability and performance. This includes:

- Real-time system health checks
- Monitoring of transaction volumes and error rates
- Performance benchmarking
- User feedback collection and issue tracking

Explore's support team remains actively engaged during the stabilization period to address any emerging issues and ensure the MCC system operates as expected.

Project Management and Governance

Explore Information Services applies a disciplined and transparent project management framework to ensure the successful delivery of the MCC IRP/IFTA system. Our governance model promotes accountability, collaboration, and continuous communication with the Oklahoma Corporation Commission (OCC) and other stakeholders throughout the project lifecycle.

Project Governance Structure

Explore establishes a clear governance structure that defines roles and responsibilities across both Explore and OCC teams. Key roles include:

- **Project Manager**: Serves as the primary point of contact, oversees day-to-day execution, and manages scope, schedule, and resources.
- **Technical Lead**: Responsible for system architecture, integration, and technical oversight.
- **Business Analyst**: Facilitates requirements gathering and ensures alignment with jurisdictional needs.

- **Quality Assurance Lead**: Oversees testing activities and ensures deliverables meet quality standards.
- **OCC Stakeholders**: Participate in planning, review, and acceptance activities, and provide jurisdictional guidance.

This structure ensures that all aspects of the project are managed effectively and that decisions are made collaboratively.

Scope Management

Scope Management ensures project scope is well defined, understood by stakeholders, documented in tangible terms and the project can be managed against that scope.

The requirements that will be used for scope management will be extrapolated from the Statement of Work and once agreed upon will be the scope of the project. The project schedule will include this scope and supporting details for project implementation.

During project execution, the Project Managers monitor work progress to ensure it supports the prioritized work products and deliverables documented in the project schedule. It is the responsibility of the Project Managers to ensure that work progresses only on items defined as "in scope." If work elements do not support prioritized work products and deliverables, this indicates the project is functioning out-of-scope. The Project Managers must initiate corrective action if the project is functioning out-of-scope. If it is not within the scope of the project, then it may be considered a change that should be handled through the Change Management process.

In order to validate that all contractual obligations have been met, a Requirement Traceability matrix (RTM) will be used during the contract duration. The matrix tracks all requirements in the Statement of Work and then will track when each is validated by either testing or design documentation.

Contract completion/fulfillment or system acceptance is when the Requirement Traceability matrix is completed. Any exclusions or exceptions noted in the matrix will be substantiated by an approved change request.

SOLERA | Explore

This document contains confidential information intended solely for internal use. Any unauthorized copying, distribution, or use for external purposes is strictly prohibited.
© 2025. All rights reserved.

BR ID	Requirement Description	Status					Deliverables / Milestones	Milestone Completion [%]	Milestone Target Date	Comments
		BRD Approved	Development	Test	Deployment	Training				
BR_Test_ID-1.00	User Interface Design: The system shall provide an intuitive and accessible user interface to support efficient task completion.	✓	✓	✓	✓		Milestone 1	0.25	04/25/20XX	
BR_Test_ID-1.01	Role-Based Access Control: The solution shall provide mechanisms for users to access the system based on defined roles and permissions.	✓	✓				Milestone 1	0.25	04/25/20XX	
BR_Test_ID-2.00	Performance Requirements: The system shall meet performance benchmarks for response time, throughput, and availability.	✓					Milestone 2	0.1	06/15/20XX	
BR_Test_ID-3.00	Security & Privacy: The solution shall protect sensitive business data in accordance with applicable standards.	✓	✓				Milestone 3	0.05	06/15/20XX	
BR_Test_ID-3.01	Functional Capability: The solution shall support core business functions necessary to meet operational objectives.	✓					Milestone 3	0.05	09/01/20XX	

Figure 6 Sample Requirements Traceability Matrix (RTM)

Explore Information Services also applies a disciplined and collaborative approach to scope control, ensuring that only essential changes are approved and that all stakeholders are informed in a timely and transparent manner.

Key tools and practices include:

- Change Control Boards (CCB) and formal change request workflows to evaluate and approve scope modifications.
- Use of Microsoft Project and other automated project tracking tools to monitor progress, dependencies, and scope boundaries.
- Checklists, stage gates, and review checkpoints to ensure quality and alignment with project objectives.
- Risk logs and mitigation plans to proactively identify and manage scope-related risks.

Explore's project teams work closely with jurisdictional stakeholders to:

- Define scope clearly during project initiation.
- Document all proposed changes with impact assessments.
- Review and approve changes through a structured governance process.
- Communicate scope changes through weekly status meetings and formal documentation.

Communication Management

The primary objectives of Communication Management are to communicate project related information to:

- Inform stakeholders about the project and its status
- Reinforce the commitment of Explore leadership to the project
- Maintain coordination between different implementation teams
- Detect misunderstandings before they impact, cost, schedule or fulfillment of objective

Informal communication such as email, individual conversations, and phone calls will be frequent and will provide early warning of potential problems. During informal communication, it is vitally important to cc both project managers in order for them to be knowledgeable on items being discussed outside of formal documented meetings.

Formal communication will be regular, as detailed in following table and will include meeting agendas, document approvals, documents shared on the project repository, updates to the published project schedule, and email status updates.

Internal

Communication Type Formal (F) Informal (I)	Communication Objective	Medium	Frequency / Duration	Content Owner	Target Audience	Deliverable
Project Kick Off (F)	• Reviews project objectives/scope review and approve • Project Management approach (governance docs/PMP) • Reviews implementation methodology and high-level timeline	On-Site	One time event	Project Manager	Project Sponsor Project Team Key Stakeholders	Presentation Mtg Minutes
Project Management Meeting (F)	• Review project scope, schedule and budget to validate milestones have been met • Validates project risks and issues have been addressed	Virtual	Weekly/ < 30 min	Project Manager	Project Management	Agenda Mtg Minutes Project Schedule
Project Status Meeting (F)	• Reviews project status with the team	Virtual	Weekly/ < 1 hr	Project Manager	Project Team	Status Report Agenda Mtg Minutes Project Schedule
Solution Meetings (SME) (F)	• Discusses, reviews and develops design or configuration solutions for the system	Virtual	Weekly 1 hour	Product Owner and Lead BA	Workstream Lead/Analysts	Agenda Meeting Minutes Action Items
Project Status Reports (F)	• Reports the status of the project. Including activities, progress, change requests, risks and issues.	Email	Weekly/ Every Wednesday	Project Manager	Project Stakeholders	Project Status Report Updated Project Schedule
Demo and Testing Meetings (F)	• Notifies testers of testing schedules, logistics, environment, scripts and reporting process.	Virtual	At the end of every milestone	Product Owner, Lead BA, and Project Manager	Project Team and Test Team	Testing process, Meeting minutes
Training Meetings (F)	• Notifies super and end users of training schedules, logistics, environment, materials and plan.	On-Site	TBD	Project Manager	Super Users End Users Workstream Lead	Training Plans, Training Schedule
Monthly Written Deliverables Reports (F)	• Monthly reports for data based on the previous month (Software defect report, Risk and Objective Report, Incident Report, Outage report)	Email	Monthly/ No later than 10^{th} calendar day of each month	Project Manager	Project Stakeholders	Monthly Status Report (upon request)

Communication Type Formal (F) Informal (I)	Communication Objective	Medium	Frequency / Duration	Content Owner	Target Audience	Deliverable
Quarterly Reports (F)	• Fiscal process improvement goals and action plans with attainment of improvement goals.	Email	Monthly/ No later than 10th calendar day of each month	Project Manager	Project Stakeholders	Quarterly Status Report (upon request)
Annual Reports (F)	• Fiscal process improvement goals and action plans with attainment of improvement goals.	Email	Quarterly	Project Manager	Project Stakeholders	Annual Report (upon request)
Downtime (Cutover), Implementation (F)	• Notifies users of upcoming downtime	Email	TBD	Project Manager	End Users Workgroup Leads Help Desk Impacted Users	GoLive Plan
Go Live (F)	• Go Live Announcement	Email	TBD	Project Manager	End Users Project Team Members Sponsor(s) Impacted Users Help Desk	GoLive Plan

Status Meetings

Explore conducts regular status meetings, typically on a weekly or bi-weekly basis, depending on the phase of the project. These meetings include:

- Progress updates on milestones and deliverables
- Review of risks, issues, and action items
- Planning for upcoming activities and stakeholder engagement

Meeting agendas and notes are documented and shared to maintain transparency and alignment.

Reporting Mechanisms

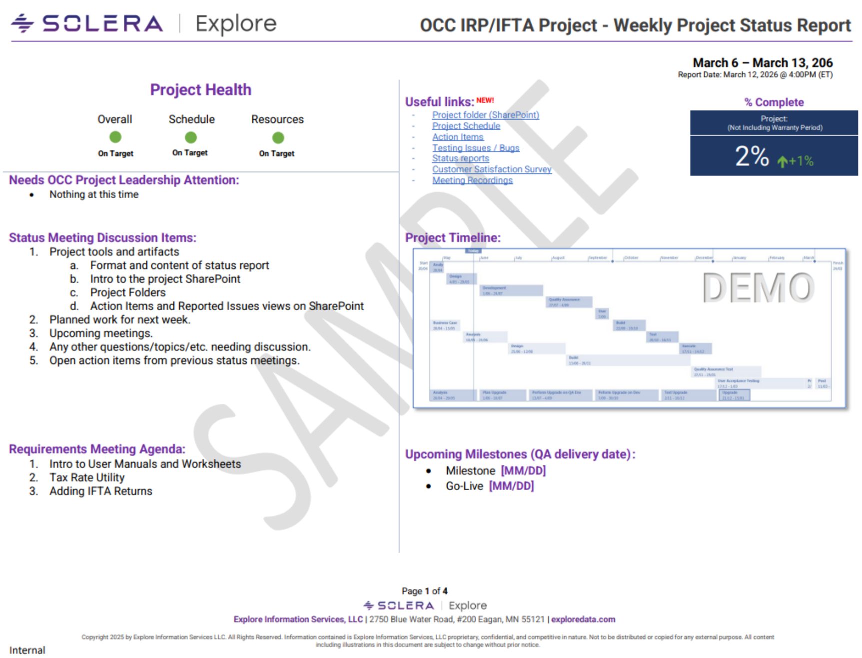
Explore provides consistent, structured, and actionable reporting to the Oklahoma Corporation Commission (OCC) through a centralized Status Report, which serves as the primary tool for communicating project progress, health, and risks.

The Status Report is designed in a dashboard-style format, offering both visual and numeric summaries of key project metrics. It includes:

- **Progress Overview**: Percentage completion of milestones and deliverables, with visual indicators for completed vs. remaining work
- **Gantt Chart View**: Timeline representation of current and upcoming activities

Internal

- **Project Health Indicators**: Color-coded status lights (Green, Yellow, Red) to reflect milestone health based on scope, schedule, and resource alignment
    - **Green**: On track — no issues impacting scope, schedule, or resources
    - **Yellow**: At risk — potential issues identified; mitigation in progress
    - **Red**: Off track — issues impacting delivery; escalation required
- **Milestone Highlights**: Summary of recently completed deliverables and upcoming targets
- **Risk and Issue Summary**: High-level view of open items, mitigation strategies, and resolution timelines



SOLERA | Explore

OCC IRP/IFTA Project - Weekly Project Status Report

March 6 – March 13, 206
Report Date: March 12, 2026 @ 4:00PM (ET)

Project Health

Overall	Schedule	Resources
On Target	On Target	On Target

Needs OCC Project Leadership Attention:
- Nothing at this time

Useful links: NEW!
- Project folder (SharePoint)
- Project Schedule
- Action Items
- Testing Issues / Bugs
- Status reports
- Customer Satisfaction Survey
- Meeting Recordings

% Complete
Project: (Not Including Warranty Period)
2% +1%

Status Meeting Discussion Items:
1. Project tools and artifacts
    a. Format and content of status report
    b. Intro to the project SharePoint
    c. Project Folders
    d. Action Items and Reported Issues views on SharePoint
2. Planned work for next week.
3. Upcoming meetings.
4. Any other questions/topics/etc. needing discussion.
5. Open action items from previous status meetings.

Project Timeline:

DEMO

Requirements Meeting Agenda:
1. Intro to User Manuals and Worksheets
2. Tax Rate Utility
3. Adding IFTA Returns

Upcoming Milestones (QA delivery date):
- Milestone [MM/DD]
- Go-Live [MM/DD]

SAMPLE

Page 1 of 4
SOLERA | Explore
Explore Information Services, LLC | 2750 Blue Water Road, #200 Eagan, MN 55121 | exploredata.com

Internal

Figure 7 Sample Weekly Status Report - Page 1

SOLERA | Explore **OCC IRP/IFTA Project - Weekly Project Status Report**

Recent Accomplishments:
- Project management tools and artifacts were set up.
- Project SharePoint was updated with new views and folders for this project
- Project schedule is being updated and it will be published on SharePoint.
- Explore worked on the first four worksheets, and will review them with the OCC team

Items Planned for Next Week:
- Complete the project schedule on MS Project
- Update project artifacts and documents based on OCC feedback
- Demo of the MCC system

Requirement Action Items: (link)
- 4 New NEW!
- 0 Ready for review by Jurisdiction
- 0 On Hold
- 0 In Progress
- 0 In Development
- 0 Ready for Explore Review
- 0 Not Ready
- 0 Requiring Approval by Jurisdiction
- 0 Approved by Jurisdiction
- 0 Complete

Testing Reported Issues / Bugs: (link)
- 0 Reported
- 0 Analyzed
- 0 Working On
- 0 Retest State Staff
- 0 Status Closed

Project RAID Log:
- 0 Status Open
- 0 Critical Severity
- 0 High Priority
- 0 Status Closed

Project Risk Log:
- Nothing defined at this time.

Project Issue Log:
- No Issues currently

Page 2 of 4

SOLERA | Explore

Explore Information Services, LLC | 2750 Blue Water Road, #200 Eagan, MN 55121 | exploredata.com

Copyright 2025 by Explore Information Services LLC. All Rights Reserved. Information contained is Explore Information Services, LLC proprietary, confidential, and competitive in nature. Not to be distributed or copied for any external purpose. All content including illustrations in this document are subject to change without prior notice.

Internal

Figure 8 Sample Weekly Status Report - Page 2

SOLERA | Explore **OCC IRP/IFTA Project - Weekly Project Status Report**

Upcoming Scheduled Meetings (next 10 days)

Date	Time (ET)	Topics	Organizer	Invitees
Mon 3/11	2:00 PM	Explore/OCC Roles/Expectation Discussion	KY	Core team
Wed 3/13	9:30 AM	Status Meeting and SME call. Topics: 1. Intro to User Manuals and Worksheets 2. Tax Rate Utility 3. Adding IFTA Returns	EXPLORE	Core team
Wed 3/20	9:30 AM	Status Meeting and SME call. Topics: 1. TBD	EXPLORE	Core team

Upcoming Holidays (next 30 days)

Name	Date(s)	Affected project activity	Notes

Project Members Out of Office (upcoming vacation or business meetings)

Team member(s)	Reason	Date Out of Office	Contact (Backup)
Explore			
Nikki	Out of the Office	3/25 – 3/29	Diana/Carlos
OCC			

Page 3 of 4

SOLERA | Explore

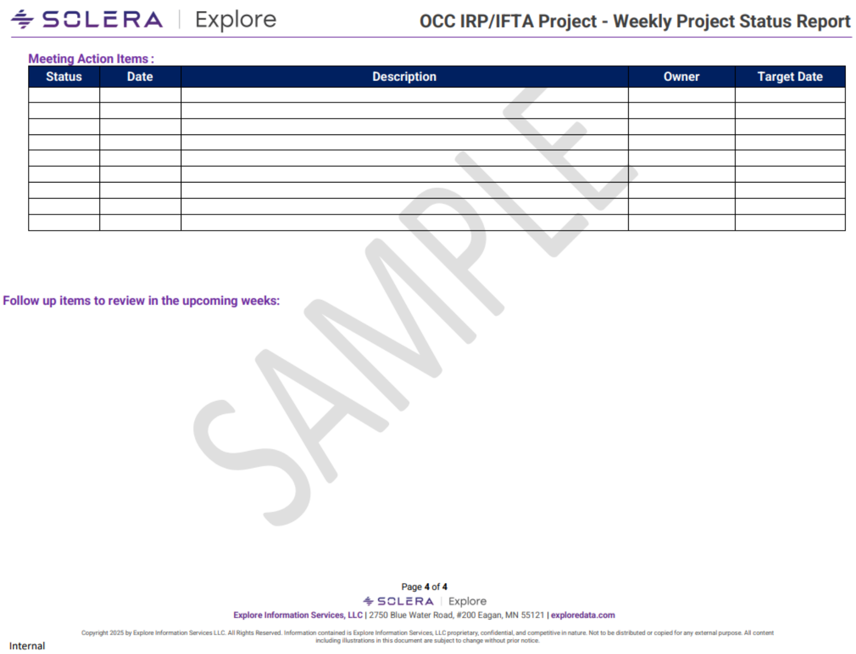
Explore Information Services, LLC | 2750 Blue Water Road, #200 Eagan, MN 55121 | exploredata.com

Copyright 2025 by Explore Information Services LLC. All Rights Reserved. Information contained is Explore Information Services, LLC proprietary, confidential, and competitive in nature. Not to be distributed or copied for any external purpose. All content including illustrations in this document are subject to change without prior notice.

Internal

Figure 9 Sample Weekly Status Report - Page 3

Internal



OCC IRP/IFTA Project - Weekly Project Status Report

Meeting Action Items :

Status	Date	Description	Owner	Target Date

Follow up items to review in the upcoming weeks:

SAMPLE

Page 4 of 4

Explore Information Services, LLC | 2750 Blue Water Road, #200 Eagan, MN 55121 | exploredata.com

Copyright 2025 by Explore Information Services LLC. All Rights Reserved. Information contained is Explore Information Services, LLC proprietary, confidential, and competitive in nature. Not to be distributed or copied for any external purpose. All content including illustrations in this document are subject to change without prior notice.

Internal

Figure 10 Sample Weekly Status Report - Page 4

Project progress data is primarily sourced from Jira, where work is organized to mirror the structure of the project schedule. This alignment allows Explore's Project Manager, who is actively involved in Agile ceremonies and has full access to Jira, to update Microsoft Project regularly, typically one to three times per week. These updates ensure that the project schedule remains current and accurately reflects real-time progress, blockers, and dependencies.

MS Project is also synced with the project's SharePoint site, where OCC stakeholders have access to a dedicated Project Schedule page for live updates and insights.

In addition to the Status Report, Explore maintains:

- A **Risk and Issue Log** to track and manage open items and escalation paths (Refer to Risk and Issue Management section for more information)
- A **Traceability Matrix** to ensure all requirements are mapped to delivered functionality and validated through testing

Explore also provides supplemental reports upon request, including:

- **Quarterly Executive Reports**: High-level summaries of project progress, risks, and key decisions for leadership review
- **Customer Feedback Reports**: Based on satisfaction surveys conducted after each milestone, these reports capture stakeholder input to guide improvements and ensure alignment with expectations

Internal

- **Change Request Logs**: Documentation of all approved or pending change requests, including impact assessments and current status
- **Requirements Traceability Reports**: Detailed mapping of requirements to delivered functionality and associated test coverage

These reporting mechanisms ensure that OCC stakeholders remain informed, engaged, and empowered to make timely decisions throughout the project lifecycle.

Requirements Gathering and Stakeholder Engagement

Explore facilitates structured requirements gathering sessions with OCC and jurisdictional representatives during each milestone. These sessions are designed to:

- Clarify business needs and operational workflows
- Identify jurisdiction-specific requirements
- Validate assumptions and document functional specifications

Stakeholder engagement continues throughout the project via review meetings, feedback loops, and collaborative planning.

Risk and Issue Management

Explore maintains a formal risk and issue management process that includes:

- Identification and documentation of risks and issues
- Assessment of impact and likelihood
- Assignment of ownership and mitigation strategies
- Regular review and escalation as needed

This process ensures that potential challenges are addressed early and do not impact project delivery.

Risk Log

High-level project risks are identified in the Risk Log (See Table 3 Risk Log). The Risk Log is located in the project repository. The necessary data fields in the Risk Log are identified in the following table:

Table 3 Risk Log

Field	Definition
ID	Risk unique identifier
Risk Type	Scope, Schedule, Budget, Resources, System Reliability, Project Management, User Adoption
Risk Description	Brief description of the risk (for a more detailed description, please add a complete description in the Additional Information tab in the RAID
Probability	Rate the probability of this risk occurring from 1 (low) to 3 (high)
Impact	Rate the impact of this risk on the risk type from 1 (low) to 3 (high)
Risk Score	This is automatically populated (Probability * Impact)
Status	Open, Closed

Internal

Field	Definition
First Indicator	When was this first indicated? (i.e. Project Kick Off)
Mitigation Approach	Mitigate (M) Avoid (A) Transfer(T) Acceptance (Ac). Watch (W)
Risk Owner	Who is responsible to mitigate this risk?
Due Date	When is this risk due?

Risk Assessment

The high-level risk assessment is an initial broad view of the risk associated with the project.

The risk assessment process includes a review and determination of whether the identified risks are acceptable. Risk assessment is not a one-time event; Project Manager will assess the risks identified weekly or more frequently if required throughout the project.

Risk Identification

During the initiation phase of the project, high-level risk information is gathered in an initial meeting of the Project Managers and the OCC Project Team members. Each Project Team member will identify and provide a list of potential risk items. As the project progresses, the team will identify and assess additional risks which will result in a complete list of potential risks of the project. The characteristics of each identified risk are captured and entered into the Risk Log (see Figure 11).

ID	Date Identified	Risk (short description)	Status	Assigned to	Resolution Date	Impact (H,M, L)	Probability (H, M, L)	Mitigate (M) Avoid (A) Transfer (T) Acceptance (Ac) Watch (W)	Mitigation Plan / Resolution	Exec. Level

Figure 11 Risk Log

Risk Analysis and Quantification

After identifying the potential risks, the project team and/or project manager reviews each risk to classify and prioritize the risk and seeks to assess the probability of occurrence and impact to the project. This risk analysis and quantification process will lead to the creation of the Risk Log. The team will manage and accept those risks deemed most likely to have a negative impact to the project.

Risk Prioritization

The prioritization of a risk is based upon the potential impact of the risk on the project and the probability of occurrence, which computes the risk exposure. The team and/or project manager will assess the risk mitigation timeframe and apply some expert judgment to determine the overall prioritization order for the risks.

Internal

The probability on the likelihood of the risk occurring (1-33%=Low Risk, 33-66%=Medium Risk, 66-99%=High Risk) while the risk is based on the impact (Low, Medium, or High) to either cost, schedule, and/or performance. Both, probability and impact are combined to determine a final rating or risk score for each risk.

Risk Response

The project team will identify the mitigation response to each of risk listed in the project Risk Log. The response can consist of one of the following responses:

- Mitigate (M) – Used to reduce the probability and/or impact of an adverse risk event to an acceptable threshold. Taking early action to reduce the probability and/or impact is often more effective than trying to repair damage if the risk occurs.
- Avoid (A) – Involves changing the project plan to eliminate the threat posed by the adverse risk.
- Transfer (T) – Requires shifting the negative impact of a threat along with ownership of the response to a third party. Transferring the risk simply gives another party responsibility for its management.
- Acceptance (Ac) – Risk acceptance involves simply accepting the risk event and its consequences. Project team and/or project manager will monitor the risk and deal with the event if it occurs.
- Watch (W) – Usually a low rating risk that needs to be monitored to validate it has not increased in probability or impact.

For each response that is accepted, a mitigation plan has been developed and is summarized in the Risk Log for that risk.

Risk Tracking and Control

The objective of risk tracking and control is to ensure that all steps of the Risk Management Procedures are being followed, and as a result, risks are being mitigated and mitigation plans are followed as necessary. Risk tracking and control involves the oversight and tracking of risk mitigation action plan execution, avoidance plan execution, reassessment of risks, reporting of risk status, and recording risk information changes in the project Risk Log.

Risk Tracking

The Project Manager is responsible for the high-level oversight of the execution of mitigation strategies for all risks identified in the project Risk Log. The Project Manager is also responsible for updating the Project Sponsor and Executive Leadership via identified and accepted communication mediums and obtaining their approval as needed.

Internal

Risk Control

The Project Manager will reassess the risk information in the project Risk Log to determine if any changes are needed. The risk probability or impact could change based upon project events or other information. Reassessment of risk information will be performed on a weekly basis, but it may be performed more frequently if needed. Risk status is included as part of the project status meetings. Risk status reporting will focus on the high-level executive ranked risks. Information presented will include the status of risk mitigation plans, changes in risk prioritization for known risks, and any new risks identified.

Issue Management

An issue is a situation, action, problem, or question arising during the performance of the project, which cannot be efficiently or effectively resolved within a project team. Left unresolved, an issue will impede or prohibit project-related progress or development by delaying or suspending a task or project. In some cases, risks that have occurred and will be moved to the Issue Log as shown in Figure 12 Sample Issue Log.

ID	Date Identified	Issue	Issue (short description)	Status	Assigned to	Resolution Date	Impact (H, M, L)	Severity (H, M, L)	Mitigation Plan / Resolution

Figure 12 Sample Issue Log

The Issue Log will be used to log and track issues and their resolutions during the project. Issues are identified and communicated to the project team and documented in the Issue Log. The necessary data fields in the Issue Log are identified in the following table:

Field	Definition
ID	Issue unique identifier
Who Reported	The project team member who reporting the issue. If it came from the Risk Log, please indicate so
Issue Summary	Brief description of the issue (for a more detailed description, please add a complete description in the Additional Information tab in the RAID)
Priority	If impact is high, priority is 1, if impact is medium, priority is 2, and if impact is low, priority is 3
Status	Open, Closed
Date Reported	Date reported to Project Management
Date Assigned	Date assigned by Project Management
Date Resolved	Date issue was resolved
Assigned To	Project team member assigned to resolve issue
Resolution	Resolution of issue

Internal

The team and/or project manager will assess the impact and apply some expert judgment to determine the overall impact for the issue. The Issue Log is in the project repository.

The Project Manager and project team leads will meet weekly for the project status meetings and will review the Issue Log and discuss possible solutions. Issues that cannot be resolved by their target resolution dates and at the team level will be escalated as follows

Figure 13 Issue Resolution Escalation Path

Change Control Procedures

Explore implements a structured change control process to manage scope adjustments and ensure alignment with project goals. This includes:

- Documentation of change requests
- Impact analysis on schedule, cost, and resources
- Review and approval by OCC and Explore leadership
- Integration of approved changes into the project plan

This governance model ensures that changes are managed responsibly and transparently.

Communication and Collaboration

Explore Information Services prioritizes clear, consistent, and collaborative communication throughout the MCC IRP/IFTA system implementation. Our approach ensures that all stakeholders remain informed, engaged, and aligned across every phase of the project.

Collaboration Tools

Explore utilizes a suite of modern tools to facilitate real-time collaboration, task tracking, and document sharing:

- **Microsoft Teams**: Used for meetings, chat-based communication, and quick coordination between Explore and OCC staff.
- **SharePoint:** Serves as the central repository for project documentation, deliverables, meeting notes, and reference materials. Explore also uses SharePoint's List feature to manage action items, track issues, and monitor project tasks collaboratively with OCC.
- **Jira:** Used internally by Explore to track development tasks, bugs, and enhancement requests. While OCC does not access Jira directly, Explore uses it to manage sprint progress and issue resolution, and shares relevant updates through meetings and documentation.

These tools enable seamless communication across teams and ensure that all project artifacts are accessible and up to date.

Internal

Communication Protocols

Explore establishes clear communication protocols with State stakeholders to support project governance and day-to-day coordination. These include:

- Defined points of contact for Explore and OCC teams
- Scheduled status meetings (weekly or bi-weekly)
- Ad hoc working sessions for requirements, testing, and issue resolution
- Email summaries and action item tracking following key meetings

Explore ensures that all communications are documented and shared promptly to maintain transparency and accountability.

Documentation and Knowledge Transfer

Explore supports long-term sustainability of the MCC system through structured documentation and knowledge transfer practices. These include:

- Functional and technical documentation for system components and configurations
- User guides and training materials tailored to OCC staff and jurisdictional users
- Knowledge base articles for common tasks and troubleshooting
- Walkthroughs and Q&A sessions during implementation and post-go-live support

Note: Refer to Section 07-05 – Explore - Documentation and Training.pdf document.

These practices ensure that OCC has the resources and understanding needed to operate and maintain the MCC system effectively.

Continuous Improvement and Feedback Loops

Explore Information Services is committed to continuous improvement throughout the development and implementation of the MCC IRP/IFTA system. Our iterative approach is designed to incorporate stakeholder feedback early and often, ensuring that the system evolves in alignment with jurisdictional needs and expectations.

Feedback Collection During Development

Explore actively collects feedback from OCC and other stakeholders during each milestone. Mechanisms include:

- Regular review sessions following each development iteration
- Hands-on access to functionality in the QA environment
- Informal feedback channels via Teams, email, and shared documentation
- Issue tracking and enhancement requests managed through SharePoint Lists

This ongoing engagement allows Explore to identify usability concerns, clarify requirements, and refine features before final deployment.

Iterative Refinement Based on Stakeholder Input

Feedback received during development is used to guide iterative refinement of the MCC system. Explore's agile methodology supports:

- Rapid adjustments to functionality based on OCC input
- Prioritization of enhancements in upcoming milestones
- Continuous validation of business rules and jurisdiction-specific workflows

This approach ensures that the system remains responsive to stakeholder needs and delivers meaningful value with each iteration.

Post-Implementation Review and Lessons Learned

After go-live, Explore conducts a post-implementation review in collaboration with OCC to evaluate project outcomes and identify opportunities for improvement. This review includes:

- Assessment of project execution and milestone delivery
- Evaluation of system performance and user adoption
- Documentation of lessons learned and recommended process enhancements

Insights from the review are used to inform future projects, refine internal practices, and strengthen Explore's delivery model.

Section Seven: Explore Documentation and Training

Documentation to Support Knowledge Transfer

Explore provides a comprehensive suite of documentation to ensure effective knowledge transfer and long-term operational success for the MCC IRP/IFTA system. These materials are designed to support both DMV staff and motor carriers and are securely maintained via the MCC SharePoint site.

System Manuals

Explore provides detailed system manuals that serve as foundational resources for understanding and operating the MCC IRP/IFTA system. These manuals are designed to support DMV staff, administrators, and technical teams by offering:

- **Comprehensive Business Rules:** Clear documentation of IRP, IFTA, and permitting rules, including system requirements and compliance standards.
- **Validation Logic:** Descriptions of system checks and automated validations that ensure data integrity and regulatory compliance.
- **Workflow Descriptions:** Step-by-step outlines of key processes such as account setup, license renewals, supplement processing, and audit workflows.
- **Functional Operations:** Detailed guidance on system functionality across modules, including user roles, permissions, and transaction flows.
- **Configurable Items:** Identification and explanation of configurable elements such as validation thresholds, permit types, jurisdiction codes, etc. These items are documented to support future system updates and customization by State administrators.

All manuals are version-controlled and securely maintained on the MCC SharePoint site, ensuring users have access to the most current and accurate information.

Help System

The MCC portal includes an embedded Help System designed to provide immediate, role-specific assistance to users. Key features include:

- **Searchable Content**: Users can quickly locate relevant guidance using keyword search.

Internal

- **Role-Based Views**: Content is tailored for staff, system administrators, and motor carriers, ensuring relevance and clarity.
- **Contextual Assistance**: Help topics are linked directly to system screens and functions, offering just-in-time support.

This system reduces dependency on external support and promotes user self-sufficiency.

Technical Specifications

Explore provides a full set of technical documentation to support IT teams and integration efforts. These specifications include:

- **Interface Definitions**: Detailed descriptions of APIs, data exchange formats, and integration points with external systems.
- **Configuration Parameters**: Documentation of system settings that can be adjusted to meet jurisdictional requirements, including:
    - Data retention policies
    - Security roles and access controls
    - Batch processing schedules
- **System Architecture Overviews**: Diagrams and narratives explaining the system's infrastructure, hosting environment, and scalability features.
- **Environment Details**: Information on development, test, and production environments, including deployment protocols and versioning practices.

These materials ensure technical teams can maintain, extend, and troubleshoot the system effectively.

Troubleshooting Guides

Explore's troubleshooting guides provide step-by-step instructions for resolving common issues encountered during system use. These guides include:

- **Error Message Resolution**: Clear explanations of system-generated errors and recommended corrective actions.
- **Process Recovery Steps**: Instructions for restarting failed transactions, correcting data entry errors, and managing incomplete workflows.
- **User Role-Specific Issues**: Troubleshooting tips tailored to IRP processors, IFTA auditors, and administrators.
- **Escalation Paths**: Guidance on when and how to escalate issues to technical support, including contact details and response expectations.

These guides are updated regularly and accessible via the MCC SharePoint site.

Quick Reference Sheets

Quick Reference Sheets are concise, task-focused guides designed to support high-frequency activities. These include:

- **Step-by-Step Instructions**: Visual walkthroughs for tasks such as trailer registration, IRP supplements, and IFTA license renewals.
- **Printable Formats**: Available as PDFs for easy distribution and desk-side reference.
- **Audience-Specific Versions**: Tailored sheets for staff, auditors, and administrators.
- **Update Notifications**: Version-controlled with update alerts to ensure users are working with the latest procedures.

These sheets help reduce training time and improve operational efficiency.

Contact Directory

Explore maintains a centralized technical support contact directory to ensure timely assistance and efficient issue resolution. Key features include:

- **Escalation Paths**: Clearly defined tiers of support, including first-level help desk contacts, system administrators, and Explore technical leads.
- **Role-Based Contacts**: Separate contact lists for staff, auditors, and administrators to streamline communication and reduce response time.
- **Availability Details**: Includes hours of operation, expected response times, and emergency support procedures.
- **Access via SharePoint**: The directory is securely hosted on the MCC SharePoint site and updated regularly to reflect staffing changes and escalation protocols.
- **Post-Go-Live Support**: Contact information for Explore's onsite support team during initial production rollout is included to assist with immediate issues.

This directory ensures that users know exactly who to contact and how to escalate issues based on severity and urgency.

User Training Approach

Explore Information Services will deliver a comprehensive, role-based training program to ensure all OCC staff are fully prepared to operate the MCC IRP/IFTA system from day one. This implementation includes onsite classroom training, supplemented by virtual and on-demand resources to support long-term knowledge retention and future onboarding.

Training Delivery Methods

- **Onsite Classroom Training**: Explore will conduct in-person sessions for approximately 20 OCC staff, including finance, audit, and system administrators. Training will be hosted at an OCC-selected facility equipped with computers, tables, and a projector.
- **Instructor-Led Sessions**: Explore trainers will lead sessions using PowerPoint presentations, live demonstrations, and hands-on exercises with test data.
- **Functional "Fast Path" Exercises**: Real-world scenarios such as processing new accounts, filing IFTA returns, and correcting unit information will be practiced to reinforce learning.
- **Training Materials**: Explore will provide printed and electronic manuals tailored to each user group (e.g., IRP processors, IFTA auditors, administrators).

Training Courses

The table below outlines a sample training curriculum designed to support OCC staff in their use of the MCC IRP/IFTA system. These courses represent a baseline structure and will be customized in collaboration with OCC to align with their specific operational roles, scheduling preferences, and learning formats. Explore will work closely with OCC stakeholders to refine course content, duration, and delivery methods to ensure optimal knowledge transfer and system readiness.

Course	Audience	Duration
MCC IRP User Training	OCC Staff	1 day
MCC IFTA User Training	OCC Staff	1 day
MCC Permit Training	OCC Staff	½ day
MCC Audit Training	OCC Auditors	1 day
MCC Financial Processing	Finance Personnel	½ day
MCC Administrator Training	System Admins	1 day

Motor Carrier & Licensing Agent Training

Explore will provide targeted training resources to support external users such as motor carriers and licensing agents. While direct training for these groups is not typically included in standard implementation, Explore offers flexible options when requested by the jurisdiction.

Training materials will include:

- **"How-To" Sheets and Visual Guides**: Step-by-step instructions for common tasks, available in both electronic and printed formats.
- **Instructional Videos**: Short, task-specific videos that walk users through system functions and workflows.
- **Train-the-Trainer Option**: If requested, Explore can deliver a train-the-trainer program to equip OCC staff with the tools and knowledge needed to educate external users effectively.

These resources are designed to be intuitive and accessible, minimizing the need for formal training while ensuring motor carriers and agents can confidently navigate the MCC system.

Knowledge Transfer

Explore's approach ensures that State staff are actively involved throughout the project lifecycle and are equipped with the technical knowledge needed for ongoing system operations.

State Staff Involvement

- **Design & Configuration**: State SMEs will participate in JAD sessions, configuration workshops, and decision-making processes.
- **Testing & Validation**: Staff will engage in release verification and UAT, with Explore providing training and support.
- **Implementation Support**: Explore will be **onsite during the first week of production** to assist with go-live activities and issue resolution.

Knowledge Transfer Components

Explore's approach to knowledge transfer ensures that State staff are equipped with the skills and understanding needed to manage and maintain the MCC IRP/IFTA system independently. Key components include:

- **Training Curriculum**: Covers operations, configuration, workflow management, system administration, and maintenance.

- **Formats**: Delivered through live sessions, one-on-one learning, on-demand modules, and printable guides.
- **Documentation**: Includes system manuals, help system access, technical specifications, and troubleshooting guides, all available via SharePoint.

Explore's commitment to knowledge transfer continues beyond go-live. We support ongoing learning and system familiarity through weekly support calls, one-off sessions to demonstrate new functionality, and refresher courses tailored to evolving user needs. This ensures that OCC staff remain confident and capable as the system grows and adapts.

Internal

Section Seven: Explore Hosted Solution

Explore MCC System Overview

The Explore MCC IRP/IFTA system is delivered as a fully hosted, Commercial Off-the-Shelf (COTS) solution using a Software-as-a-Service (SaaS) model. All infrastructure is managed by Explore Information Services, LLC and hosted in secure, U.S.-based data centers.
The system is designed for ease of access and usability:

- Accessible through standard web browsers without the need for proprietary client software or plug-ins
- Users may require common desktop applications such as Microsoft Excel, Word, and a PDF viewer for specific tasks including audit file uploads, reporting, or correspondence

This architecture ensures a streamlined user experience while minimizing technical dependencies and simplifying deployment across jurisdictions.

System Architecture and Hosting Environment

The Explore MCC IRP/IFTA system is deployed in a multi-tier architecture consisting of dedicated web, application (middle-tier), and database servers. This structure supports separation of concerns, scalability, and optimized performance across all layers of the system.

Key architectural and hosting features include:

- **Virtualized Infrastructure:** All servers are virtualized using VMware vSphere ESXi, enabling rapid provisioning, resource optimization, and simplified disaster recovery.
- **Load Balancing and Redundancy:** Two web servers and two application servers are deployed in a load-balanced configuration to ensure fault tolerance and high availability. The system is designed with no single point of failure for critical components.
- **Automatic Failover:** In the event of a server failure, traffic is automatically redirected to active servers. Failover is completed in under one minute, and session state is preserved where applicable to maintain a seamless user experience.
- **Hosting Environment:** The system is hosted in the Switch data center in Las Vegas, the only Tier 5 facility on the planet, featuring a concurrently maintainable infrastructure. A geographically separated disaster recovery (DR) site is maintained in Utah to ensure continuity in case of primary site disruption.
- **Scalability:** The platform supports incremental hardware upgrades to accommodate increased usage demands without service interruption.
- **Uptime Commitment:** Explore guarantees 99.9% system availability, excluding planned maintenance windows.
- **Real-Time Monitoring:** The hosting environment includes real-time monitoring and alerting systems to proactively detect and respond to performance or availability issues.

This architecture ensures that the MCC IRP/IFTA system remains resilient, scalable, and consistently available to users across jurisdictions.

Availability, Monitoring, and SLA Commitments

Explore Information Services is committed to delivering a highly available and resilient MCC IRP/IFTA system designed to support 24/7/365 operations. The solution is hosted in the Switch data center, which features a concurrently maintainable infrastructure to ensure service continuity, even during planned maintenance or unexpected component failures.

To maintain consistent performance and reliability, Explore employs real-time monitoring and alerting systems that proactively detect and respond to issues. The system is engineered to meet uptime expectations of greater than 99%, excluding scheduled maintenance windows.

Explore will work collaboratively with the contracting agency to define a tailored Service Level Agreement (SLA) that includes:

- Clearly defined response and resolution times for incidents
- Performance benchmarks such as uptime, latency, and throughput
- Regular reporting on system performance and availability metrics

Explore can provide system reports tailored to agency needs. These may include:

- Latency statistics to monitor system responsiveness
- User access logs including identity, IP address, timestamps, and access history
- Security logs covering authentication, authorization events, alerts, and audit trails

All reports are delivered securely and retained in accordance with applicable agency policies and contractual requirements.

Security and Compliance Framework

Explore's hosting environment is governed by a comprehensive Information Security and Data Protection (IS & DP) framework aligned with federal and industry standards. This framework ensures the confidentiality, integrity, and availability of data across all system components and hosting environments.
Explore's infrastructure is hosted within the Switch data center, which features a concurrently maintainable architecture to support high availability and operational resilience. While Explore does not currently hold formal FedRAMP certification, its security practices are aligned with equivalent federal standards. Contractual assurances are provided for third-party hosting environments to meet government client expectations.

Certifications and Audits

Explore and its hosting partners maintain a robust set of certifications that validate their commitment to security and compliance:

- **ISO 27001**: Adopted across all Solera companies as the reference standard for security practices
- **SOC 2 Type II**: Independently audited annually to verify the effectiveness of internal controls
- **Additional Hosting Partner Certifications**:
    - SOC 1 Type II
    - PCI DSS
    - ISO 9001:2015
    - ISO 22301
    - ISO 14001:2015
    - ISO 50001
    - OHSAS 18001

Security Controls

Explore enforces a defense-in-depth strategy through layered security controls across administrative, technical, and organizational domains:

- **Administrative Controls**:
    - Formalized security policies and procedures
    - Security awareness and training programs for all personnel
    - Vendor risk management and third-party assurance processes
    - Documented incident response and escalation protocols
- **Technical Controls**:
    - Role-Based Access Control (RBAC) with least privilege enforcement
    - Multi-Factor Authentication (MFA) for system access
    - Encryption of data in transit (TLS 1.2) and at rest (AES-256) within a FIPS 140-2 validated cryptographic module
    - Endpoint protection and centralized monitoring via EDR solutions
    - Regular vulnerability scanning and patch management
- **Organizational Controls**:
    - Dedicated Information Security and Privacy teams
    - Governance, Risk, and Compliance (GRC) oversight
    - Business continuity and disaster recovery planning
    - Secure Software Development Lifecycle (SDLC) practices

Monitoring and Tools

Explore's security operations are supported by a 24/7/365 Security Operations Center (SOC) and a suite of monitoring tools that provide visibility into system health and security posture:

- **Crowdstrike**: Endpoint detection and response
- **Icinga**: Infrastructure and service monitoring
- **New Relic**: Application performance monitoring

Internal

- **Contrast Security**: Runtime application self-protection and vulnerability detection

Explore also performs regular vulnerability scanning and applies critical patches within 60 days of release, or sooner if risk dictates.

Data Protection and Privacy

Explore implements robust data protection measures aligned with NIST 800-53 Revision 4 and industry best practices to ensure the confidentiality, integrity, and availability of Personal and Non-Public Information (PNPI) across the MCC IRP/IFTA system.

Data Handling and Encryption

- Separate databases per jurisdiction are maintained, each with independent security controls to ensure data isolation and minimize cross-jurisdictional risk.
- Encryption standards include TLS 1.2 for data in transit and AES-256 for data at rest, ensuring strong protection against unauthorized access.
- Daily full backups and hourly transaction log backups are performed and replicated to a disaster recovery site to support data availability and integrity.
- Secure data destruction is conducted in accordance with NIST guidelines and Solera's internal policies to ensure proper disposal of sensitive information.
- Audit logging is enforced across all system components, with logs monitored by Explore's Security Operations Center (SOC) to detect and respond to anomalies.

Compliance and Certifications

Explore's hosting infrastructure is aligned with federal standards and maintained in U.S.-based data centers that hold the following certifications:

- SOC 2 Type II
- ISO 27001
- PCI DSS

These facilities are subject to regular audits to validate ongoing compliance with security and privacy requirements.

For more information on data center certifications and compliance, refer to:

- https://www.switch.com/compliance/
- https://www.databank.com/compliance-enablement/

Business Continuity and Disaster Recovery

Explore Information Services, LLC maintains a comprehensive and well-documented Business Continuity and Disaster Recovery (BC/DR) strategy to ensure uninterrupted service delivery and data protection for the MCC IRP/IFTA system. This strategy is designed to maintain system availability in the event of natural disasters, hardware failures, cyber incidents, or other disruptions.

Internal

BCP and DR Strategy Overview

Explore's formal BC/DR Plan outlines the company's approach to maintaining system operations and restoring services. The plan includes:

- Defined policy objectives and scope of applicability
- Roles and responsibilities for internal teams and hosting partners
- Disaster recovery architecture and compliance protocols
- Testing procedures and review cycles to validate effectiveness

The MCC system is hosted in a virtualized environment within the Switch data center, which features a concurrently maintainable infrastructure and geographically diverse failover capabilities. In the event of a disruption at the primary data center, services can be rapidly restored through automated backup, replication, and disaster recovery protocols.

Recovery Objectives and Testing

Explore's recovery objectives are aligned with industry best practices and can be tailored to meet contractual requirements:

- Recovery Time Objective (RTO): 24 hours
- Recovery Point Objective (RPO): 2 hours

Annual disaster recovery tests are conducted to validate the effectiveness of failover strategies and confirm adherence to RTO/RPO targets. The most recent test, conducted in July 2025, confirmed full recovery of all in-scope production application functionality within the required RTO of eight hours.

Infrastructure and Backup Technology

All servers are virtualized using VMware, enabling rapid recovery, scalability, and efficient resource utilization. Backup and recovery operations are managed through an enterprise-grade solution that provides automated, policy-driven protection for applications and data. Backups are encrypted and stored in secure, geographically redundant locations to ensure both confidentiality and availability.

Explore's backup methodology uses snapshot-based techniques to minimize system impact during backup windows. Event logs and incident forms are maintained and reviewed following any recovery operation to support continuous improvement and operational resilience.

Backup Schedule and Retention

Explore employs a layered backup strategy to minimize data loss and support rapid recovery:

- Full database backups are performed weekly
- Incremental backups occur every 2 hours
- Server and application configuration files are backed up weekly, with daily incremental backups

Backup data is stored locally on disk within the primary data center and replicated to a secondary data center to ensure redundancy and disaster recovery readiness. Retention schedules include:

Internal

- Daily backups retained for 30 days
- Weekly backups retained for 90 days
- Monthly backups retained for 1 year

This schedule supports compliance with data retention policies and ensures recovery options across multiple timeframes.

Redundancy Measures and Resilience

Explore's infrastructure is designed to eliminate single points of failure and support operational resilience through:

- Cross-training of personnel
- Remote work strategies
- Secure hosting at Switch with backup replication to Databank
- Encrypted transfers between geographically separated data centers

Disaster Recovery Planning Methodology

Explore's DR planning methodology is based on industry best practices and includes:

- Business Impact Analysis (BIA) to assess critical systems
- Defined RTO, RPO, and Maximum Tolerable Period of Disruption (MTPD) for each service
- Oversight by a Crisis Management Team (CMT)
- Emergency hardware deployment within 3–4 hours for critical systems

Recovery procedures cover both State-owned and vendor-managed data. Scenarios such as ransomware, hardware failure, and data corruption are addressed through documented DR protocols. The solution includes the option to store collected data exclusively at the vendor's site, using secure, geographically separated data centers.

Licensing and Cost Considerations

Explore's proposal includes all necessary licensing to support failover, replication, and disaster recovery. No additional software license fees are charged solely for redundancy or business continuity. This approach ensures that continuity capabilities are built into the base solution cost, aligning with expectations for cost-effective and resilient service delivery.

Source Code Escrow

Explore Information Services, LLC recognizes the importance of long-term system sustainability and risk mitigation for government clients. To support these objectives, Explore is prepared to participate in a formal Source Code Escrow arrangement upon request.

Under this arrangement:

- Explore will deposit the source code for the MCC IRP/IFTA system with a mutually agreed-upon, independent third-party escrow agent.
- Deposits will include all necessary components to compile, configure, and deploy the

Internal

system, including documentation, build scripts, and configuration files.
- The escrow agreement will define clear release conditions, such as vendor bankruptcy, acquisition, or failure to support the system as contractually obligated.
- Escrow deposits will be updated regularly to reflect major releases and critical updates, ensuring the codebase remains current and usable.
- The escrow process will comply with applicable legal and contractual requirements, and Explore will work collaboratively with the contracting agency to define terms that meet operational and legal expectations.

This approach ensures that the agency retains access to the system's source code in the event of unforeseen circumstances, supporting continuity of operations and long-term system viability.

Incident Response and Change Management

Explore Information Services, LLC follows documented procedures for managing security incidents and system changes to ensure operational stability, traceability, and compliance.

Incident Response

Explore maintains a proactive incident response framework aligned with NIST and ISO standards. This includes:

- 24/7/365 monitoring by Explore's Security Operations Center (SOC)
- Timely notification to the State in the event of a security incident or system disruption
- Escalation protocols that follow industry best practices for containment, investigation, and resolution

This approach ensures rapid detection and response to potential threats, minimizing impact on system availability and data integrity.

Change Advisory Board (CAB) Process

All changes to the MCC IRP/IFTA system are governed by a formal Change Advisory Board (CAB) process. This structured workflow ensures that changes are reviewed, approved, and implemented with minimal risk. Key elements include:

- Risk assessment and approval workflows for all proposed changes
- Version control using GIT, with rollback capabilities to maintain system integrity and traceability
- Documentation and tracking of all changes for audit and compliance purposes

The CAB process supports transparency, accountability, and alignment with agency expectations for change governance.

Maintenance and Patching

Explore maintains a proactive maintenance schedule to ensure system reliability, security, and performance. This includes:

- Monthly Windows patching and scheduled software upgrades
- Critical patches applied within 60 days of release, or sooner if risk dictates
- Staging environment testing for all updates prior to production deployment to ensure compatibility and minimize disruption

This disciplined approach to maintenance ensures that the MCC system remains secure, stable, and responsive to evolving requirements.

Support and Maintenance for Vendor Hosted System

Explore Information Services, LLC provides a comprehensive support and maintenance plan for the MCC IRP/IFTA system to ensure secure, reliable, and scalable operations. The plan includes structured release cycles, proactive monitoring, and responsive support aligned with agency requirements and industry best practices.

System Maintenance

Hardware

The MCC system is hosted in a secure, vendor-managed data center environment. Hardware is monitored 24/7 and supported by the hosting provider with automated failover and redundancy. All components are maintained by their manufacturers, and critical patches are applied within 60 days of release.

Software

- **Major Releases**: Delivered quarterly, introducing new features and enhancements
- **Minor Releases**: Deployed as needed to address urgent issues
  All releases follow a formal change management process, including testing, stakeholder communication, and rollback procedures.

Database

Monthly patching ensures security and performance. Daily backups are retained per agency policy. Monitoring tools track performance and detect anomalies.

Help Desk Support

Explore's Help Desk is available:

- 24/7 for emergencies
- Monday–Friday, 7 AM–6 PM CT for non-emergencies

Support Channels: Phone, email, and ServiceNow issue ticketing system
Updates: Provided via weekly jurisdiction meetings, email, or phone
Ticketing System: ServiceNow tracks reported issues, status, and resolution progress

Software Defect Classification

Explore uses six severity levels to prioritize and respond to reported issues:

- **P1**: System outage – Immediate response

- **P2**: Multiple users blocked – Response within 30 minutes
- **P3**: Single user blocked – Response within 4 hours
- **P4**: Issue with workaround – Response within 24 hours
- **P5**: Questions/report requests – Response within 24 hours
- **Project**: Enhancement requests – Response within 24 hours

Escalation and Emergency Procedures

Emergency issues are escalated immediately to Tier 3 support. A designated escalation path ensures rapid resolution, with updates provided throughout the incident lifecycle.

Support Task Types and Frequency

Explore performs the following support tasks on a regular basis:

- Daily system monitoring
- Weekly jurisdiction meetings
- Monthly patching and maintenance
- Quarterly major releases
- As-needed minor releases and hotfixes

Support Models

Explore offers a tiered and collaborative support structure:

- **Tiered Support**: Tier 1 (basic), Tier 2 (technical), Tier 3 (development)
- **Proactive Monitoring**: Alerts and automated diagnostics
- **Collaborative Support**: Weekly meetings with agency staff

Troubleshooting Large-Scale Failures

Explore collaborates with the agency to:

- Track mean time between deficiencies
- Diagnose root causes
- Identify repeat issues using analytics and ticket history

Maintenance Call Documentation

Each service call includes:

- Nature and status of deficiency
- Action plans and timestamps
- Expected vs. actual completion
- Resolution details
- Responsible party
- Work order number
- Reporter identity

Emergency Maintenance Notifications

Explore sends high-priority emails to agency users detailing:

- Nature of the issue
- Estimated resolution time
- Workarounds (if available)
- Ongoing updates until resolution

Hosting Infrastructure Support

All hardware and software components are supported by their manufacturers.

- **Windows Servers:** Patched monthly via SCCM
- **Patch Schedule:** Non-production on Tuesdays; production on the last Thursday of each month
- **Critical Updates:** Applied within 60 days of release

State Collaboration and Compliance

Explore Information Services, LLC is committed to maintaining full compliance with applicable Federal and State laws, regulations, and operational standards. Collaboration with government agencies is a core component of Explore's implementation and support strategy for the MCC IRP/IFTA system.

Industry Participation and Standards Alignment

Explore actively participates in national and regional working groups to ensure alignment with evolving regulatory and operational standards, including:

- International Registration Plan (IRP)
- International Fuel Tax Agreement (IFTA)
- Performance and Registration Information Systems Management (PRISM)
- Commercial Vehicle Information Systems and Networks / Intelligent Transportation Systems Deployment (CVISN/ITD)

This engagement ensures that Explore remains informed of industry trends, regulatory updates, and best practices relevant to motor carrier systems.

Structured Release Planning and Compliance Management

Explore follows a structured release planning process to manage compliance-related changes. This includes:

- Reviewing regulatory updates and business rule changes
- Scheduling and implementing updates through formal release cycles
- Coordinating with agency stakeholders to ensure timely and accurate deployment

Agency Collaboration and Support

Explore works closely with agency teams throughout the system lifecycle to ensure successful implementation and ongoing support. This includes:

- Business requirements gathering to inform system configuration and development
- Development and configuration coordination to align technical solutions with operational needs
- User Acceptance Testing (UAT) support to validate functionality and ensure readiness for production

Continuous Monitoring of Best Practices

Explore's Global IT teams continuously monitor industry best practices and emerging technologies to ensure the MCC IRP/IFTA system remains secure, scalable, and compliant with current standards.

Section Seven: Supplier Experience

Explore's Experience

Explore Information Services, LLC, a member of the Solera family of companies, brings a proven IRP/IFTA solution and deep motor carrier prorate experience to the Oklahoma Corporation Commission. While Explore serves a broad range of markets, including insurance, fleet, and commercial data services, the Government Solutions team within Explore is exclusively focused on delivering motor carrier systems to state agencies.

Explore launched its first IRP/IFTA system implementation in 2002, and since then has successfully delivered IRP/IFTA solutions in numerous jurisdictions, including Maine, Delaware, Michigan, Massachusetts, Minnesota, Texas, South Dakota, New Hampshire, Nevada, and Kentucky, as well as the IFTA Processing Consortium, which included six states (original IPC jurisdictions: California, Connecticut, Kentucky, Michigan, Maryland, New Hampshire). These implementations have ranged from legacy platform deployments to modernized solutions built on Explore's latest technology stack.

In 2020, Explore introduced Motor Carrier Connect (MCC), a Commercial-Off-The-Shelf (COTS) IRP/IFTA solution designed to meet the evolving needs of state motor carrier programs. MCC was developed through a multi-year effort involving jurisdictional focus groups and service providers, with consultation facilitated through NATSA (North American Transportation Services Association), and third-party design experts. The system supports IRP, IFTA, Permitting, and Intrastate Operating Authority, and features a mobile-friendly, responsive design for access via tablets and smartphones. Its workflow-driven architecture and jurisdiction-level configurability allow states to tailor the system to their specific operational needs.

Explore's IRP/IFTA solutions help states manage their commercial fleet clients efficiently and securely, while improving compliance and public safety. MCC automates the apportionment of credits, fees, and taxes, supports funds netting, and includes Dynamic Task Management, allowing over 700 system tasks to be configured in real-time by state administrators. Additional features include document management, audit integration, and dashboard reporting.

Explore's implementation methodology is comprehensive and flexible. The company provides business analysis, data conversion, system configuration, training, and post-deployment support. For Oklahoma, Explore proposes a hybrid collaboration model, conducting most requirements gathering and Joint Application Design (JAD) sessions remotely via Microsoft Teams or similar platforms, with periodic on-site visits to align with key milestones. This approach ensures effective communication, resource utilization, and continuity of staffing throughout the project.

The implementation team will be led by Nikki Benz, Government Solutions Product Owner, who has overseen IRP/IFTA implementations across nearly all Explore deployments. Supporting Nikki is a high-level project team comprising experienced leads in project management, business analysis,

Internal

and development. This dynamic team structure allows Explore to deploy skilled professionals as needed, ensuring flexibility and responsiveness to evolving project requirements.

Representative Projects

Explore Information Services, LLC has successfully delivered IRP/IFTA system implementations across a range of jurisdictions, consistently meeting project timelines and budgets while modernizing legacy systems and enhancing operational capabilities. Below are four representative projects that demonstrate Explore's ability to deliver scalable, configurable, and user-friendly solutions tailored to state-specific needs.

Maine Bureau of Motor Vehicles – IRP, IFTA, and Permits Modernization

Explore has supported the Maine Bureau of Motor Vehicles since 2008, providing long-term system stability and continuous modernization. In 2024, Explore implemented IRP, IFTA, and Permitting solutions for Maine, transitioning from legacy systems to the Motor Carrier Connect (MCC) platform. The modernization included full data conversion, configuration of MCC features, and integration with Maine's external systems.

Explore delivered comprehensive implementation services including onsite training, user acceptance testing (UAT), and go-live support. The MCC system now provides Maine with a mobile-friendly, configurable platform that supports IRP, IFTA, and permitting workflows.

- **Client Reference:**
  Nikki Bachelder
  Director, Division of Vehicle Services
  Bureau of Motor Vehicles
  29 State House Station, Augusta, ME 04333
  Office: 207-624-9191
  Email: Nikki.Bachelder@maine.gov
  Refer to Section 11 for Business Reference information

South Dakota Department of Revenue – IRP and IFTA Modernization

Explore partnered with the South Dakota Department of Revenue to modernize its IRP and IFTA systems by migrating from Explore's legacy platform to MCC. South Dakota has been an Explore customer since 2008. The project included interface redesign, configuration of MCC's new features, and full data conversion. Explore also enhanced South Dakota's existing interfaces to improve system performance and integration with external systems.

The implementation included onsite training, UAT coordination, and post-deployment support. The MCC system now provides South Dakota with a streamlined, mobile-accessible platform that supports both IRP and IFTA operations. The project was completed on schedule and within budget.

Internal

- **Client Reference**:
  Darrin Gerry, Revenue Supervisor
  South Dakota Department of Revenue
  Phone: (605) 367-7942
  Email: darrin.gerry@state.sd.us
  Refer to Section 11 for Business Reference information

Kentucky Transportation Cabinet – IRP, IFTA, and Intrastate Fuel Tax

Explore's relationship with the Kentucky Transportation Cabinet (KYTC) began in 2014 with the implementation of the IFTA Processing Consortium (IPC), which brought six jurisdictions live within 12 months, all on schedule and within budget. Since then, Explore has continued to expand and modernize Kentucky's motor carrier systems.

In 2020, Explore implemented Kentucky's IRP system and merged it with the state's IFTA data into the MCC platform, allowing carriers and taxpayers to manage both programs within a single system. In 2024, Explore also implemented Kentucky's Intrastate Fuel Tax program, fully integrated into MCC. Each project included data conversion, custom interface development, onsite training, UAT, and full lifecycle support. All projects were delivered on schedule and within budget.

- **Client Reference**:
  Tom McDaniel
  Director – Division of Motor Carriers
  Kentucky Transportation Cabinet
  Phone: (502) 782-7845
  Email: Tom.McDaniel@Ky.gov
  Refer to Section 11 for Business Reference information

Texas Department of Motor Vehicles – IRP and Commercial Intrastate Registration

Explore has supported the Texas Department of Motor Vehicles since 2006, providing long-term system stability and continuous enhancements. Most recently, Explore modernized Texas's IRP and Commercial Intrastate Registration systems by transitioning from its legacy platform to the Motor Carrier Connect (MCC) system. This modernization included configuring MCC to support new features, enhancing state programs and interfaces, and performing full data conversion.

Explore delivered comprehensive implementation services including onsite training, user acceptance testing (UAT), and go-live support. The project was delivered on schedule and within budget, and the MCC system now provides Texas with a mobile-friendly, configurable platform that supports both IRP and intrastate registration workflows.

- **Client Reference**:
  Carol Fallin
  Texas Department of Motor Vehicles

Internal

Phone: (800) 299-1700
Email: Carol.Fallin@TxDMV.gov
Refer to Section 11 for Business Reference information

Program Manager Qualifications

Explore proposes Nikki Benz as the Program Manager for the Oklahoma IRP/IFTA project. With over 19 years of experience in IRP/IFTA system implementations, Nikki Benz has consistently demonstrated her ability to lead complex, multi-jurisdictional projects from inception through post-implementation support. She has served as Principal Product Owner and Business Systems Analyst across nearly all Explore deployments, including those in Texas, Delaware, Maine, Michigan, Massachusetts, Minnesota, Kentucky (and IPC), New Hampshire, Nevada, and South Dakota.

Her leadership style emphasizes strategic vision, stakeholder engagement, and cross-functional coordination. She has overseen requirements gathering, testing, training, and deployment activities, ensuring alignment with state-specific regulations and business needs. Nikki Benz holds sufficient authority within Explore to coordinate across departments and prioritize the Oklahoma project as needed.

References for Program Manager

1. **Darrin Gerry**
   South Dakota Department of Revenue
   Phone: (605) 367-7942
   Email: darrin.gerry@state.sd.us

2. **Latasha Williams**
   Kentucky Transportation Cabinet
   Phone: (502) 564-1257
   Email: LatashaF.Williams@ky.gov

3. **Omer Guzman**
   Michigan Department of Treasury
   Phone: (517) 636-0711
   Email: guzmano@michigan.gov

Internal

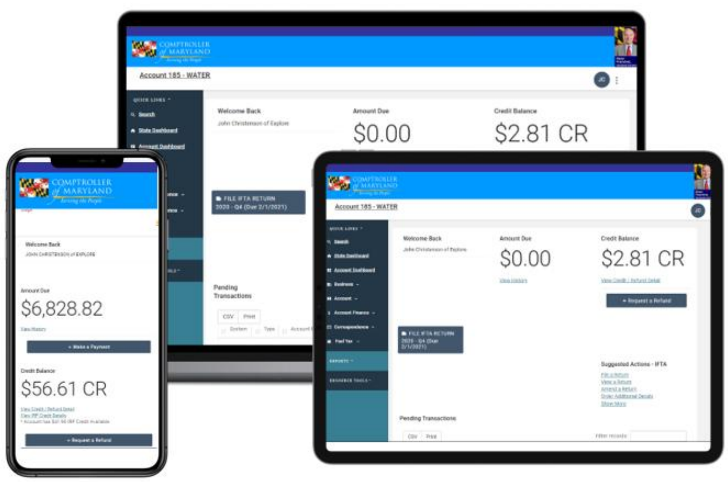
Explore Motor Carrier Connect (MCC) Product Literature

Table of Contents

Description Of Solution

Explore is proposing Motor Carrier Connect (MCC) as our Commercial-Off-The-Shelf (COTS) based solution for IRP and IFTA processing. MCC is built using a human-centered design, ensuring intuitive navigation and minimal training requirements for both agency staff and motor carriers. MCC uses a unified code base and offers high configurability at the jurisdiction level which enables jurisdictions to tailor the system to meet specific operational and regulatory requirements.

MCC represents the culmination of a multi-year endeavor aimed at developing the most adaptable and user-friendly IRP/IFTA solution for jurisdictions. Valuable input and feedback from jurisdiction focus groups, licensing agencies, and an external design firm have played a pivotal role in shaping MCC's development. The Explore MCC solution will be tailored to meet the specific business requirements of the Oklahoma Corporation Commission.



To ensure maximum accessibility and convenience, Explore MCC has been developed as a responsive web application, accessible across a range of devices including tablets and mobile phones. The design supports flexible administration and usage while maintaining full compliance with WCAG 2.1 accessibility standards.

Explore MCC delivers a comprehensive suite of motor carrier compliance functions, including IRP, IFTA, and Permits. Its intuitive dashboard interface enables users to manage compliance efficiently from any device, ensuring a seamless experience whether accessed via laptop, tablet, or smartphone.

Fully aligned with the requirements of IRP, IFTA, Audit Procedures Manual, and PRISM plans, MCC provides comprehensive functionality to facilitate compliance processes. Upon logging in, state users are directed to the State Dashboard, where they can administer tasks and functions related to IRP, IFTA, and Permitting systems. The system also includes flexible search tools to easily locate relevant information such as accounts, licensing agencies (aka service providers), decals, payments, invoices, vehicles, and credentials. Additionally, the QUICKLINKS menu offers convenient access to a range of resource tools within the system.

Internal

Core Functional Areas

Explore MCC supports a wide range of motor carrier compliance functions, including:

- **Account Management**: Centralized dashboard with alerts, contact/address books, legal status flags, payment plans, and notes management.
- **Restriction Management**: Table-driven status codes with cascading restriction logic and cumulative deny point visibility.

IRP Functionality

Explore MCC provides comprehensive support for IRP operations, offering tools and workflows that streamline fleet management, jurisdictional compliance, financial processing, and audit readiness.

- **Fleet & Vehicle Management**: Supports IRP fleet types, multi-unit changes, vehicle exchanges, bulk uploads, and state registration system integration for registration alignment.
- **IRP Workflow Management**: Unified supplement structure, collaborative editing, renewal widgets, and statewide title and registration systems data synchronization.
- **Weight Group Management**: Configurable weight groups with validation and audit logging.
- **Jurisdiction Management**: Mileage checks, non-contiguous jurisdiction validation, and historical trend analysis.
- **IRP Financial Processing**: Fee calculation engine, multi-method payments, certified funds enforcement, and state finance system integration like OCC's IMS.
- **Credit Management**: Escrow, overpayment, deposit, and application credits with auto-reserve logic and refund workflows.
- **Finance Exceptions**: Payment removal with audit trail and state system interface updates.

IFTA Functionality

Explore MCC provides comprehensive support for IFTA operations, offering configurable tools and workflows that streamline return processing, jurisdictional compliance, financial reconciliation, and audit readiness.

- **License Management:** License applications, renewals, and decal orders
- **Returns Management:** MCC supports online filing with jurisdiction-specific validation, automated tax calculation, and error handling to ensure accurate and timely submissions. In addition, the system allows XML/CSV return uploads for bulk or assisted filing, applying late filing interest and penalties, and generating payment instructions to streamline financial processing.

Internal

- **Late Filing Interest and Penalty Configuration:** Jurisdiction-specific rules for interest and penalties applied to late filings.
- **IFTA Financial Processing:** Seamlessly integrates with the state's financial systems and payment processor to support transactions including payments, refunds, and adjustments.
- **Credit Management:** Credit management and write-offs with audit trail and approval workflows.

Audit Management

MCC includes a robust audit module for IRP and IFTA, supporting:

- Full audit lifecycle with stratification and selection tools
- Automated notifications and appeal workflows
- Audit invoice generation and reversal tracking
- Annual activity reporting and compliance documentation

Administration & Security

MCC enforces separation of duties through granular security roles and tasks. State administrators manage user roles, and all actions are logged for audit purposes. The system supports dynamic configuration of permissions and utilities for maintaining user accounts and security policies.

Inventory & Document Management

MCC provides robust tracking and management of IRP plates, decals, and consignment inventory. The system supports both automated and manual assignment workflows, multi-office tracking, and inventory location management. Through configurable settings and role-based user authority, trusted carriers and service providers can manage their own consignment inventory, such as plates, and assign them directly to fleets. This delegated model improves operational efficiency while maintaining oversight and control.

The system also includes intelligent document upload capabilities. Based on workflow steps and jurisdiction-specific business rules, MCC can determine which documents are required for submission. Documents uploaded by external users, such as carriers or service providers, are automatically queued for review and approval by state personnel. To support long-term storage and compliance, MCC can integrate with the state's system of record to store uploaded documents securely and consistently.

Additional features include:

- Real-time inventory visibility across jurisdictions and office locations
- Dashboard alerts for outstanding materials and pending actions
- Audit logging for inventory transactions and document handling

Communications & Reporting

MCC supports dynamic system-generated correspondence using customizable templates that can be tailored to jurisdictional requirements. The system allows for office address mapping to ensure accurate routing and branding of communications. Correspondence can be triggered by workflow events, user actions, or system conditions, and includes support for email, print, and downloadable formats.

Reporting capabilities are designed to meet both operational and analytical needs. MCC includes:

- **Standard Reports**: Predefined reports for common operational tasks and compliance tracking.
- **Scheduled Reports**: Automatically generated reports delivered at configured intervals.
- **Ad Hoc Reports**: On-demand reporting with flexible filters and export options.
- **Easy Query**: A streamlined interface that empowers users to build and run custom queries through guided selections and intuitive tools, making data exploration accessible without requiring technical expertise.
- **Role-Based Access Controls**: Ensures users can only access reports and data appropriate to their permissions, maintaining data security and integrity.

These tools provide jurisdictions with the flexibility to monitor system activity, analyze trends, and support decision-making across IRP and IFTA programs.

Clearinghouse Transmittals and PRISM Compliance

MCC automates both daily and monthly transmittals to the IRP and IFTA Clearinghouses, ensuring timely and accurate data exchange. For IFTA, the system supports daily demographic file generation and both Transmittal Option 1 and Option 2 for returns and audit data, aligning with IFTA Inc. specifications.

To support PRISM compliance, MCC includes:

- US DOT and TIN validations to ensure carrier identity accuracy
- SAFER-compliant transaction sets for standardized data exchange
- Credential issuance restrictions based on PRISM safety status
- PRISM-specific reports and correspondence to support enforcement and monitoring

These capabilities ensure MCC meets federal and jurisdictional requirements for motor carrier safety, registration, and tax reporting.

Account Management

The Account Dashboard serves as the central hub for initiating IFTA and IRP functions, making payments, viewing credits, and requesting refunds within the Explore Motor Carrier Connect (MCC) system. It provides important alerts and notifications to ensure timely actions, such as reminders

Internal

to renew a fleet, file an IFTA return, or fulfill required materials. The dashboard also displays account transactions in a pending status, allowing users to track their progress.

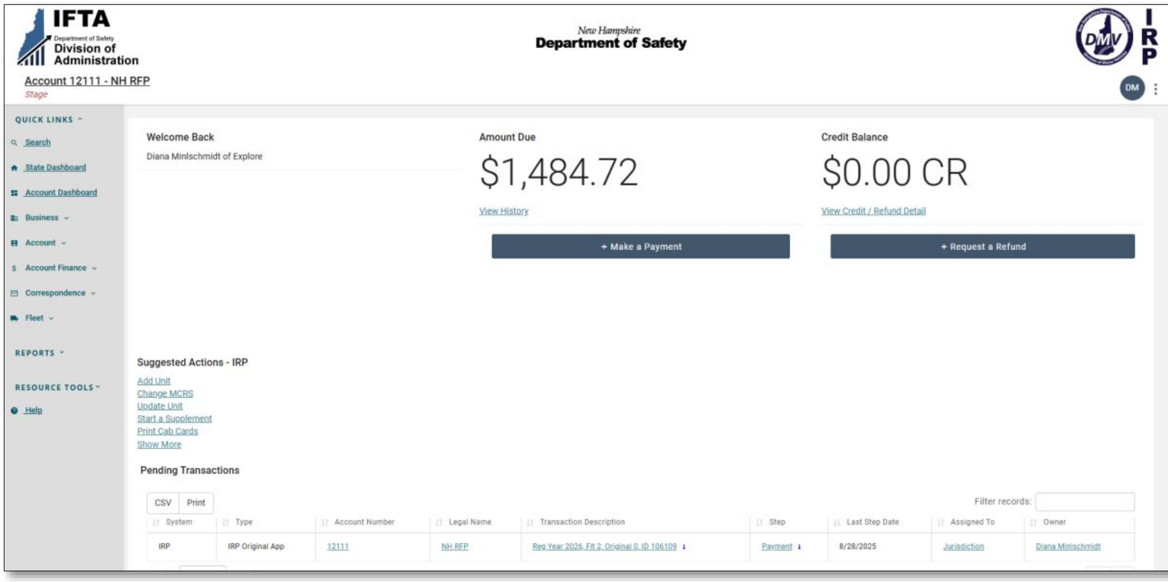


Figure 1: MCC Account Dashboard

To streamline contact and address management, the system includes dedicated Contact and Address books. Contacts can be assigned multiple contact types, including officer roles and audit representatives, while addresses can be categorized by type, such as physical, mailing, or shipping. Each contact can be associated with one or more addresses, allowing for flexible and accurate representation of registrant information. The system also supports address verification and standardization. Additionally, specific address types can be configured to enter a pending status when updated by external users, requiring review and approval by staff with appropriate authority. Authorized state users can configure maintenance preferences for accounts, contacts, officers, security settings, restrictions, related accounts, and notes. This level of customization ensures secure and tailored management of registrant data. These include:

- Certified Funds selection and through date for which certified funds are required.
- IFTA and IRP Preferred Distribution Method (Email/Mail) and Preferred Distribution Recipient.
- Customer Service Representative, which allows you to optionally assign staff members to specific accounts.
- Legal Status flags an account going through bankruptcy and suppresses the delinquency process for IFTA returns.
- Payment Plan(s) establishment. Unique payment plans with amortization schedules can be generated for each payment plan in an account.
- IFTA Contiguous Jurisdiction and IFTA MPG Rules override at the account level.

Internal

- Related Account(s) establishment. Accounts can be associated with other account(s) when they share a common identifier such as such as officer name or officer driver's license number.
- Bonds management allows you to require, track, and maintain bonds.
- Note Management enables state users, with authority, to add comments to Accounts. Notes are maintained at many levels.

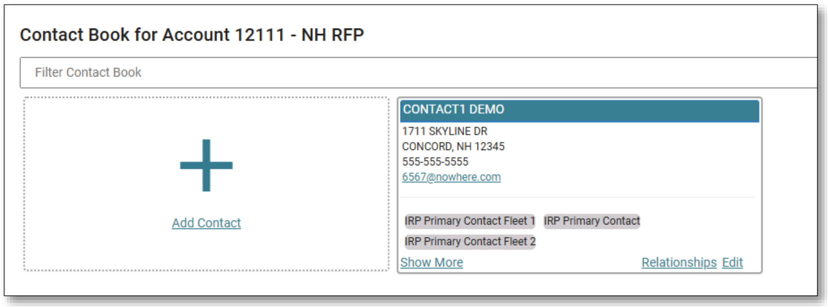


Figure 2: Contact Book

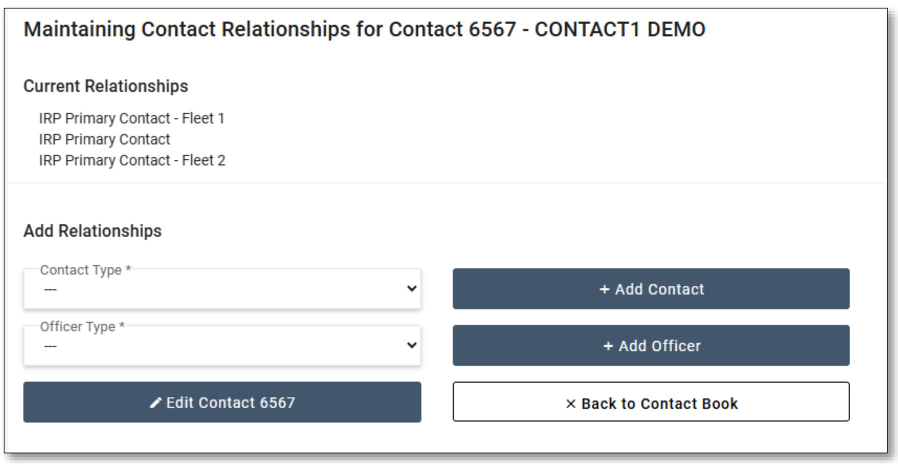


Figure 3: Maintaining Contact Relationships

Restriction Management

With MCC, restriction management is handled comprehensively to ensure compliance and enforce business rules. The system maintains table-driven status codes that are configured to trigger specific restrictions, such as suspensions, based on predefined business rules. These status codes can be customized for different jurisdictions, while still aligning with the requirements of IRP, IFTA, and PRISM requirements.

One of the key features of MCC's restriction management is the ability to configure downstream effects for each restriction. This means that when a restriction is applied, it can have a cascading impact on other related processes or functions within the system. State users have the ability to view cumulative restrictions, providing them with a clear overview of the deny points associated with the applied restrictions. This allows for better visibility and understanding of the restrictions' implications. An example of this can be seen in the scenario of an IRP revocation being added, where the cumulative restrictions and deny points would be displayed to the state users.

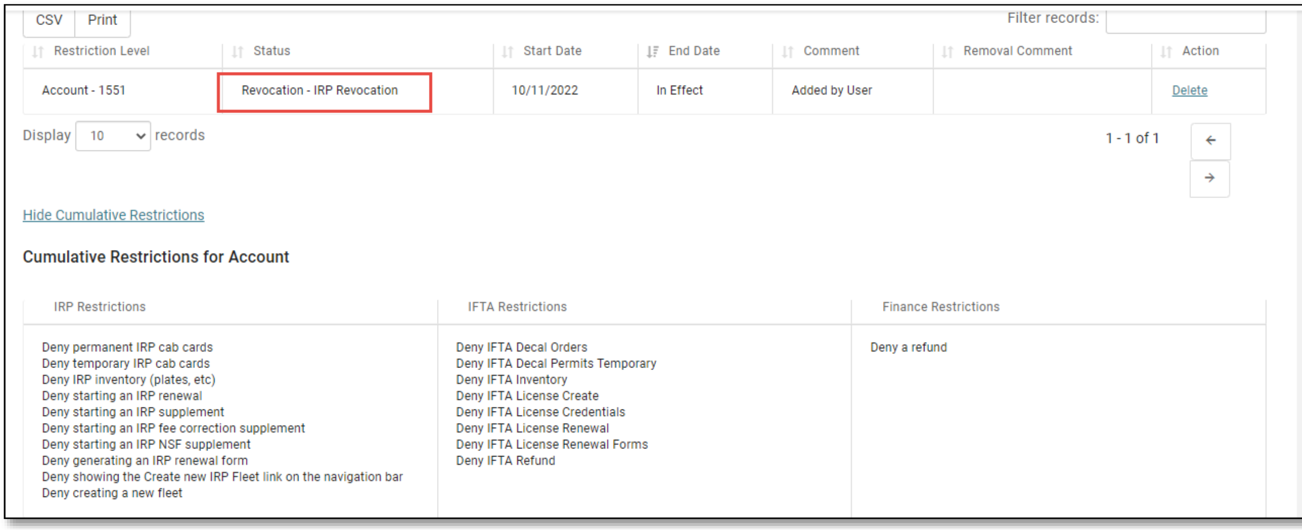


Figure 4: Restrictions Management Utility

Fleet Management

MCC provides IRP Fleet Management. IRP Fleet Types include:

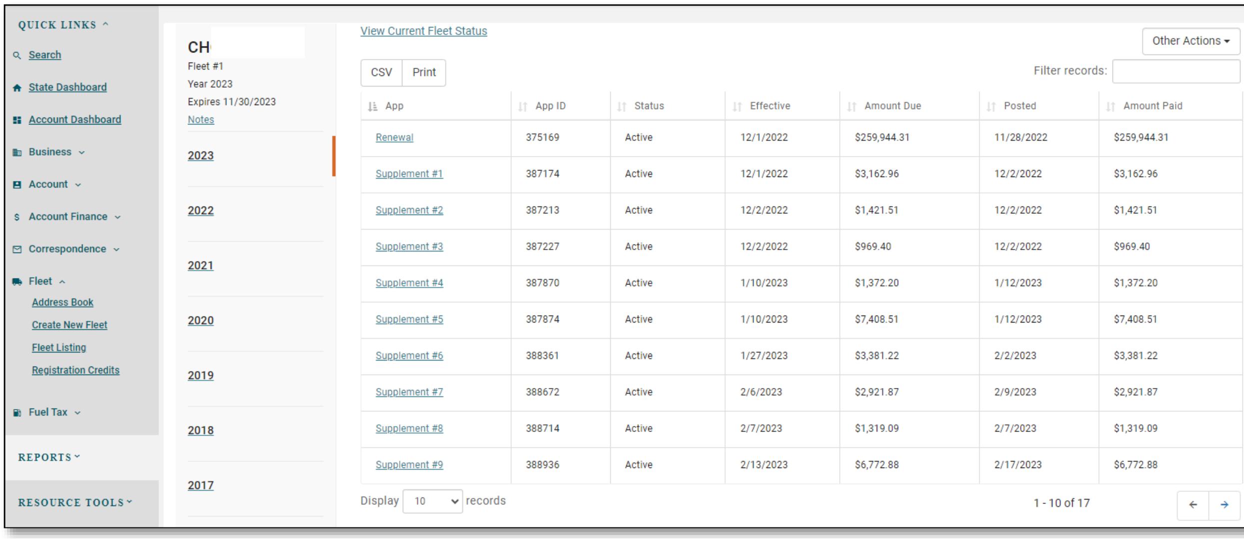
- Apportioned for Hire
- Apportioned Private

Fleet Uses include:

- Standard
- Household Goods

An IRP Fleet may be copied to another Fleet during the Fleet Creation process. Each customer fleet may have a unique description, contacts, address and office location preference (for multi-location environments). This provides flexibility to direct correspondence to the fleet level.

A complete history of all transactions, per fleet, is available by registration year.



App	App ID	Status	Effective	Amount Due	Posted	Amount Paid
Renewal	375169	Active	12/1/2022	$259,944.31	11/28/2022	$259,944.31
Supplement #1	387174	Active	12/1/2022	$3,162.96	12/2/2022	$3,162.96
Supplement #2	387213	Active	12/2/2022	$1,421.51	12/2/2022	$1,421.51
Supplement #3	387227	Active	12/2/2022	$969.40	12/2/2022	$969.40
Supplement #4	387870	Active	1/10/2023	$1,372.20	1/12/2023	$1,372.20
Supplement #5	387874	Active	1/10/2023	$7,408.51	1/12/2023	$7,408.51
Supplement #6	388361	Active	1/27/2023	$3,381.22	2/2/2023	$3,381.22
Supplement #7	388672	Active	2/6/2023	$2,921.87	2/9/2023	$2,921.87
Supplement #8	388714	Active	2/7/2023	$1,319.09	2/7/2023	$1,319.09
Supplement #9	388936	Active	2/13/2023	$6,772.88	2/17/2023	$6,772.88

Figure 5: Fleet History

IRP Process/Workflow Management

Explore's Motor Carrier Connect (MCC) solution provides comprehensive IRP Application Processing designed to streamline registration workflows and enhance operational efficiency. The system supports a wide range of activities within a single supplement, including unit additions, exchanges, weight changes, and credential replacements. This unified approach simplifies the user experience and reduces administrative overhead.

MCC promotes collaboration by allowing multiple users to work on the same supplement simultaneously. Supplements can be saved in an "in progress" state, enabling users to pause and resume work without data loss. In cases where corrections are needed, authorized staff can un-file supplements to make necessary adjustments. Additionally, MCC includes specialized supplement types such as Retraction Supplements and Fee Correction Supplements to address errors identified after the daily close process.

To ensure consistency with the base jurisdiction's internal systems, MCC integrates with the state's title and registration system to support seamless data exchange. Where supported by the jurisdiction, MCC can perform real-time inquiries against the title and registration system during key vehicle transactions, such as adding a unit, to validate existing data and reduce entry errors. Once the registration process is completed within MCC, the system can transmit finalized registration details back to the state's title and registration system, ensuring alignment across platforms

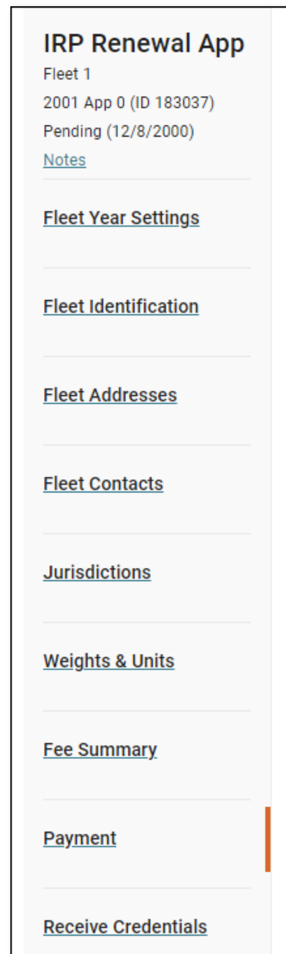


Figure 6: IRP Renewal Workflow

Internal

and maintaining accurate, up-to-date records. This integration enhances operational efficiency and provides a unified experience for both users and administrators.

When it is time to renew an IRP fleet, users are notified based on their preferred communication method. MCC supports multiple notification channels, including email and printed letters, allowing the base jurisdiction to configure communication preferences according to policy or operational needs. Additionally, SMS messaging is being introduced as a newly developed option, offering jurisdictions greater flexibility in how renewal alerts are delivered. Jurisdictions may choose to enable or disable any combination of these methods, such as relying solely on mailed correspondence if desired.

Upon accessing the Account Dashboard, users are presented with a dedicated Renew widget that guides them through the renewal process. This widget is configurable and supports the base jurisdiction's requirement to notify users in advance of the renewal period. The notification lead time (e.g., up to X months) is a configurable value provided by the state, allowing jurisdictions to tailor the timing to their operational needs. The renewal workflow is designed to be intuitive and efficient, reducing administrative burden and improving compliance.

Figure 7: IRP Renewal Widget Reminder

Workflows are provided for

- Original IRP Applications
- IRP Renewals
- IRP Applications/Supplements for, but not limited to:
  - Vehicle Exchanges
  - Multi-Unit Updates
  - Fleet to Fleet Vehicle Transfers
  - Extending Temporary Registration for Vehicle
  - Changing MCRS
  - Bulk Vehicle Upload
  - Weight Changes
  - Credential Replacements

Workflow steps can be assigned to internal and external users.

Weight Group Management

Motor Carrier Connect (MCC) supports robust Weight Group Management for IRP fleets. Vehicle weights are organized into configurable weight groups at the fleet level, and each unit is assigned to a specific group. In addition to group weights, MCC maintains unladen weight directly on the vehicle record to support jurisdictional compliance and reporting.

All weight modifications are performed through standard IRP application workflows, including renewals and supplements. During these transactions, users can create, update, or reassign weight groups, and move units between groups as needed. MCC enforces jurisdictional weight limits by triggering validation errors when a selected weight exceeds the maximum allowed by a jurisdiction. Additionally, MCC applies a 10% weight variance validation to ensure that vehicle weights remain within acceptable thresholds when compared to the assigned group, helping prevent misclassification and ensuring regulatory accuracy.

Maintaining weight groups and vehicle records is security task driven by application type, ensuring that only users with appropriate authority can perform these updates. All changes are logged for audit purposes, supporting transparency and regulatory compliance.

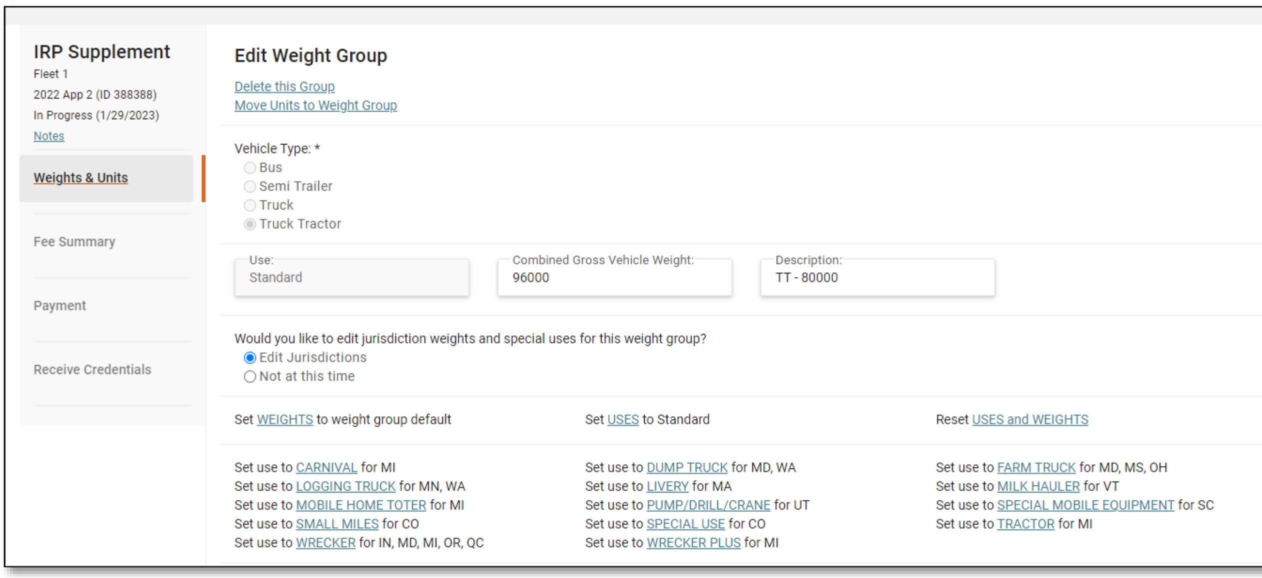


Figure 8: Maintain Weight Group page

Vehicle Management

MCC includes Vehicle Management to facilitate the handling of vehicle data. To ensure consistency with the base jurisdiction's internal systems, MCC supports an inquiry function that retrieves unit-specific information from the state's title and registration system. This feature allows authorized users to view and resolve any discrepancies between MCC and the jurisdiction's system. Once updates are made and the application is complete in MCC, MCC can transmit the revised registration information back to the state title and registration system, maintaining alignment and supporting accurate, up-to-date records.

When maintaining units in MCC, the system performs validation checks to verify the Motor Carrier Responsible for Safety (MCRS) USDOT number as part of its compliance with PRISM (Performance and Registration Information Systems Management) program requirements. MCC supports real-time validation through a live API call to the SAFER (Safety and Fitness Electronic Records) database, ensuring that the USDOT number is active and associated with a legitimate motor carrier. Additionally, MCC maintains a local copy of SAFER target files, updated daily, which allows for efficient lookups and redundancy in case of API unavailability. This dual validation approach supports safety enforcement, data accuracy, and alignment with federal standards.

By leveraging this integration and validation, MCC streamlines the vehicle management process and ensures that the system contains accurate and up-to-date vehicle data for compliance and reporting purposes.

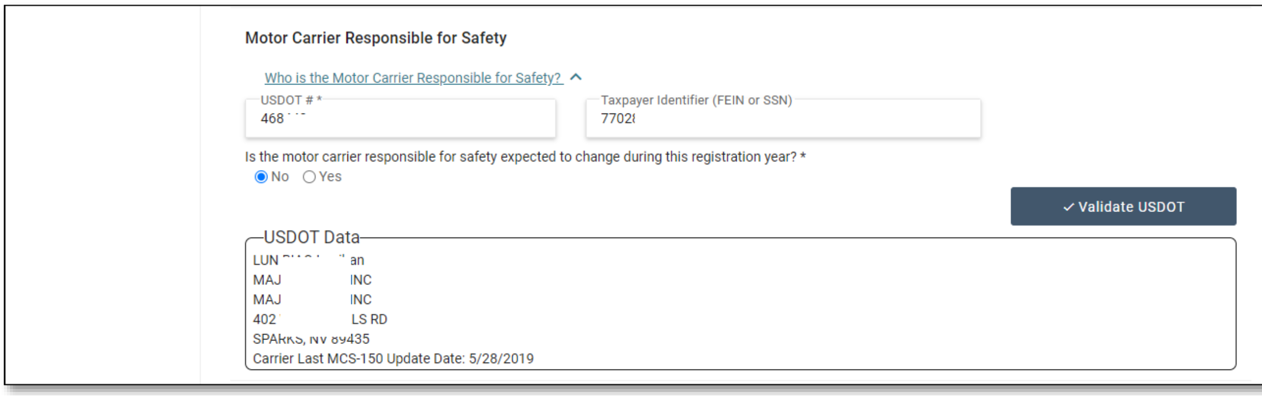


Figure 9: USDOT Data validation on the Unit page

MCC provides a convenient multi-unit change feature that allows users to modify the same data, such as the MCRS USDOT number and Tax ID, for multiple units simultaneously. This feature saves time and effort by eliminating the need to update each unit individually.

In the case of a unit exchange, MCC allows the user to select the specific unit from which to transfer credits and, if permitted by the base jurisdiction, credentials. This streamlined process simplifies the exchange procedure and ensures that relevant credits and credentials are properly transferred between units.

MCC supports bulk vehicle uploads using a standardized file template, enabling users to efficiently import large volumes of vehicle data in a single operation. This feature is especially beneficial for managing large fleets or integrating data from external sources. The bulk upload process applies the same comprehensive data validation rules used during manual vehicle entry. Any vehicles that fail validation are flagged within the application, allowing users to review and correct errors directly. Upon completion of the upload, the system automatically notifies the user via email with a summary of the results, ensuring transparency and timely follow-up.

By offering these features, MCC enhances efficiency and productivity in vehicle management tasks, making it easier for users to handle multiple units, perform exchanges, and manage vehicle data in bulk.

Internal

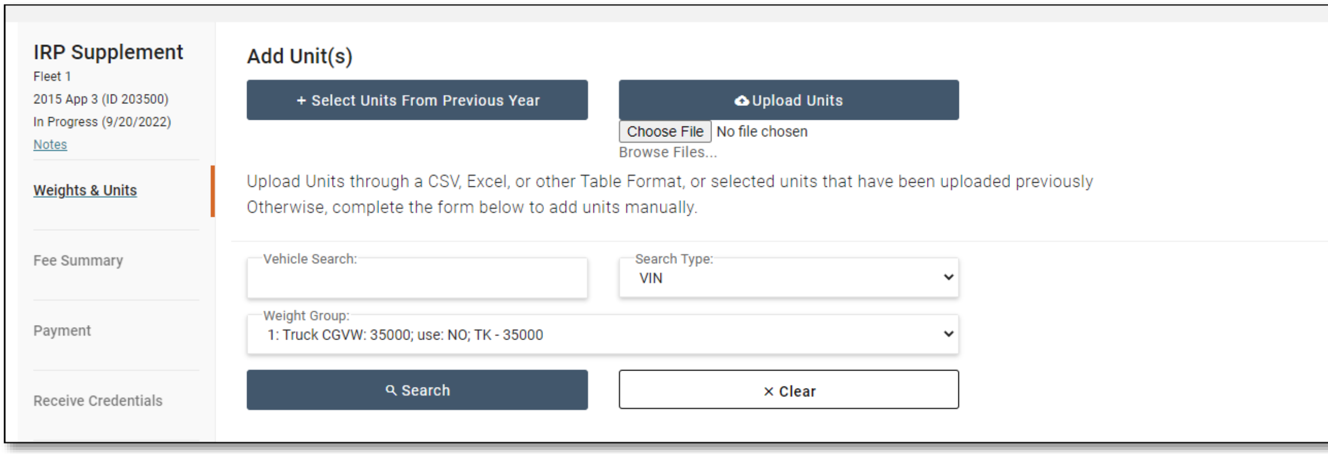


Figure 10: Add unit options

Jurisdiction Management

MCC offers robust IRP Jurisdiction Management capabilities to support accurate mileage calculation and reporting for IRP accounts. For accounts with a single fleet, MCC allows users to leverage IFTA-reported miles to automatically populate IRP jurisdiction mileage totals. This integration streamlines data entry, reduces manual effort, and ensures consistency between IFTA and IRP reporting. By pulling mileage directly from the account's IFTA data, MCC helps maintain alignment across programs and supports more efficient and reliable jurisdictional reporting.

To strengthen data integrity and support accurate fee calculations, MCC incorporates robust validation mechanisms, including irregular distance and non-contiguous jurisdiction checks. The system flags applications where reported distances appear anomalous, such as identical mileage reported across all jurisdictions when compared to the prior year or two years prior, prompting staff review before finalization. These checks do not halt the application process; carriers may proceed through fee calculations while flagged data is under review. Additionally, MCC verifies that reported mileage aligns with the jurisdictions involved, accounting for non-contiguous or atypical routing scenarios. This dual-layered approach helps identify inconsistencies and potential fraud, ensuring compliance and promoting trust in the registration process.

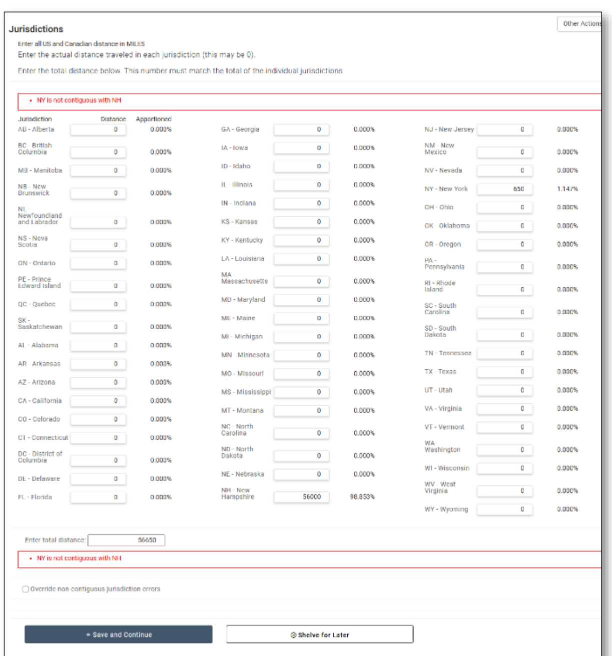


Figure 11: Contiguous jurisdiction error on the Jurisdiction page

Internal

IRP Fee Calculations

Motor Carrier Connect (MCC) features a robust and highly configurable fee calculation engine that accurately computes registration fees for both base and foreign jurisdictions. The engine leverages the official IRP fee schedules and jurisdiction-specific rules published by IRP, Inc., ensuring full compliance with current regulatory requirements.

Through our Service Maintenance Agreement, Explore continuously monitors and maintains all jurisdictional fee schedules, including updates to base jurisdiction fees. This proactive approach ensures that all fee changes are promptly reflected in the system, minimizing errors and delays in the registration process.

Each year, MCC supports the IRP Annual Fee Test by executing comprehensive local test runs. We provide detailed results and documentation to our customers, assist them in conducting their own jurisdictional tests, and support the submission of results to IRP, Inc. Our team closely monitors outcomes and engages directly with foreign jurisdictions when clarification or validation is needed, ensuring accuracy and consistency across all fee calculations.

IRP Financial Processing

The Financial Module within MCC serves as a core system for managing payments, batches, account credits, and fund balances. Payment Processing functionality enables taxpayers to make online payments, while staff members can post payments received over the counter or by mail. Multiple invoices can be paid at once using a single payment, streamlining the payment process for both carriers and staff members. Explore also provides a custom interface to integrate with the base jurisdiction’s payment portal or credit card swipe device, ensuring seamless payment transactions.

All fees collected within MCC are mapped to the appropriate revenue stream fund as designated by the base jurisdiction. The system supports flexible fund allocation, allowing one or more fees to be assigned to a single fund or distributed across multiple funds as needed. This configuration can be applied during invoice generation, enabling jurisdictions to tailor fund management to their financial policies. Additionally, payments made on IRP applications can be seamlessly transmitted to the base jurisdiction’s finance system, ensuring accurate reconciliation and integration with existing financial workflows.

MCC supports a variety of payment methods, including cash, check, and integration with external payment systems, all of which can be configured based on the base jurisdiction’s requirements. The system allows invoice payments to be split across multiple payment types, offering flexibility for both users and administrators. Within MCC, payment types are categorized as either certified or non-certified. When an account is flagged for non-sufficient funds (NSF), MCC automatically enforces restrictions by disallowing non-certified payment methods and requiring certified funds for future transactions. In such cases, clear messaging is displayed on both the Account Dashboard and associated invoices, informing the customer of the certified payment requirement.

Internal

This functionality ensures compliance with jurisdictional financial policies and promotes secure, accurate payment processing.

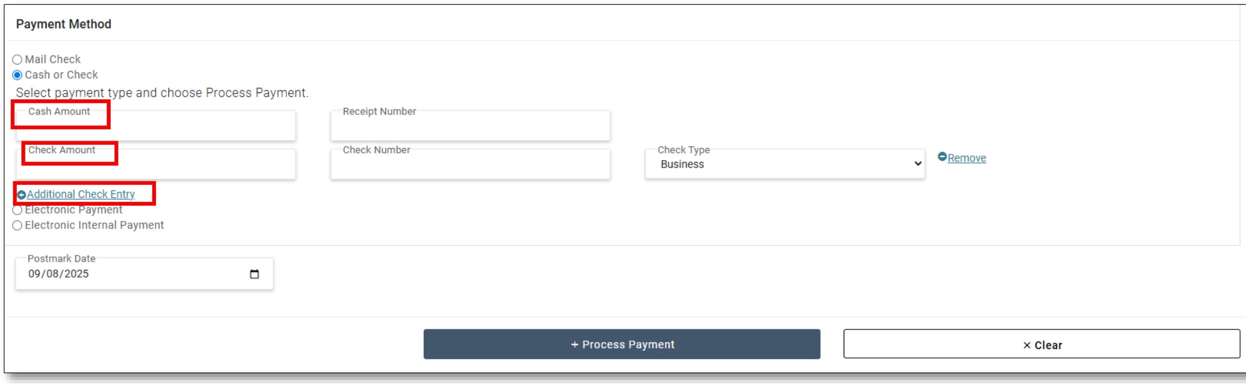


Figure 12: Split Payment Method Example

Finance Credit Management

MCC provides comprehensive credit management capabilities for IRP applications, supporting multiple credit types that are maintained outside of the IRP fee calculation process. These credits are generated and applied after applications have been filed and invoices have been generated. They are distinct from credits calculated during the IRP application process, such as those resulting from deleted units, transfers/exchanges, or weight changes, which are governed by jurisdiction-specific credit rules published by IRP, Inc.

The following finance credit types are maintained within MCC:

- **Escrow Credit:** Generated when an invoice is marked as unpaid after the daily financial batch has been closed.
- **Overpayment Credit:** Created when a payment exceeds the invoiced amount.
- **Deposit Credit:** Manually added or withdrawn by authorized users as financial adjustments.
- **Commercial Registration to IRP Credit:** Applied when transitioning from commercial registration to IRP.

MCC credit management provides the following:

- Maintaining finance credits at the account or fleet level
- Automatically reserving applicable credits when an application is filed and the invoice is generated
- Applying credits to specific invoices
- Managing credit refund requests
- Removing reserved credits from invoices when necessary

When generating invoices for filed IRP applications, MCC can automatically reserve available account credits for jurisdictions that have opted into this feature. The system follows a configurable

Internal

hierarchy to determine which credits to apply, typically prioritizing overpayment credits, followed by escrow, deposit, and then IRP application credits.

Finance Exceptions

In the MCC system, payments can be removed by an authorized user under two distinct scenarios:

1. **After the Payment Has Been Deposited**
   If a payment has already been deposited into the finance system but needs to be removed, MCC allows authorized users to perform this action following established financial procedures. Once removed, the payment amount is applied to the account's escrow credit, making it available for future use.

2. **Before the Payment Is Deposited**
   If a payment is still in process and has not yet been deposited, it can be removed based on the finance batch status. In this case, the payment is voided within the system, and no credit is applied to the account. This ensures that only finalized payments impact account balances and credit availability.

In both scenarios, when a payment is removed from the system, MCC can send an update to the state's title and registration system and/or finance system, ensuring that external systems remain in sync. A comprehensive audit trail is recorded within MCC, capturing all relevant details of the payment removal transaction. This audit trail promotes transparency and accountability by documenting who performed the action, when it occurred, and the reason for removal. The recorded information supports effective tracking and auditing, providing a clear and reliable history of payment-related activities within the MCC system.

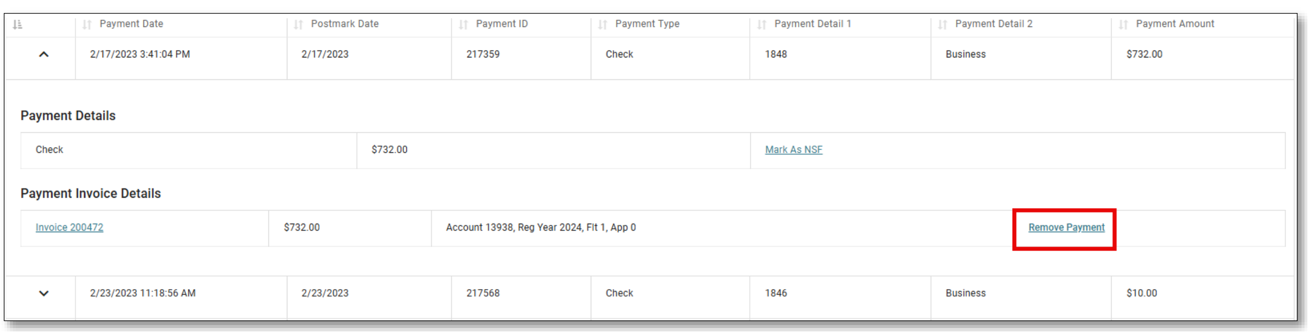


Figure 13: Remove Payment option from Payment History page

IFTA Process/Workflow Management

The base jurisdiction's participation in the International Fuel Tax Agreement (IFTA) is fully supported by MCC, which offers a comprehensive and secure platform for managing all aspects of IFTA compliance. MCC provides robust functionality for license applications, decal orders, quarterly return filing, financial processing, and audit management. The system supports automated transmittals to the IFTA Clearinghouse, ensuring timely and accurate data exchange between jurisdictions. Built-in audit tools help streamline compliance reviews and support enforcement activities. MCC also facilitates jurisdictional collaboration through standardized data formats and secure communication protocols.

Figure 14: IFTA Return Workflow Steps

To further support compliance, MCC includes a configurable delinquency notification process that allows the base jurisdiction to define when and how delinquent accounts are notified. Notifications can be triggered based on jurisdiction-defined thresholds and delivered via email, printed correspondence, or SMS, ensuring timely outreach and promoting resolution before enforcement actions are required.

These features promote operational efficiency, reduce administrative burden, and ensure consistent adherence to the IFTA Articles of Agreement, delivering a unified experience for both agency staff and motor carriers.

MCC promotes collaboration by enabling multiple users to work on the same application or return simultaneously. Returns can be shelved and saved in an "in progress" state, allowing users to pause and resume work without risk of data loss. Taxpayers benefit from automated email notifications when quarterly filings are due and can conveniently e-file their returns by logging into the system. MCC supports both email and printed letter notifications, giving the base jurisdiction flexibility to configure communication preferences, such as disabling email alerts and relying solely on mailed correspondence if desired. With the addition of SMS, this communication framework is further enhanced, supporting broader outreach and improved user engagement. Return forms are dynamically generated as PDF files for each account, streamlining the filing process and ensuring consistency across submissions.

When it's time to renew an IFTA license or file an IFTA return, the MCC system displays alerts and provides dedicated widgets on the Account dashboard. Users can simply select the relevant widget to initiate the relevant workflow, guiding them through the necessary steps.

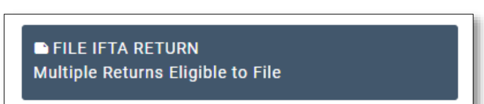


Figure 15IFTA Quarterly Return Reminder Widget

Explore MCC incorporates front-end edits to ensure the accuracy of quarterly fuel tax returns for all fuel types. These edits include validations for mileage range, net zero enforcement, and contiguous jurisdictions, helping to prevent errors and ensure compliance with IFTA requirements.

The MCC system provides a powerful and flexible upload feature that supports efficient IFTA return submission for both individual taxpayers and licensing agents (also known as service providers). Sole taxpayers can upload their own returns using a single XML or CSV file, while service providers can submit returns for multiple taxpayer accounts in one consolidated upload. The system accommodates multiple accounts, reporting quarters, fuel types, and jurisdictions within a single submission, streamlining the filing process for all users. This functionality significantly reduces manual data entry, minimizes errors, and improves accuracy, enhancing operational efficiency for both taxpayers and base jurisdictions.

Additionally, the system offers flexible configuration options for applying late filing and payment interest, as well as penalties. These settings allow the base jurisdiction to enforce its specific regulatory requirements, ensuring that penalties are assessed appropriately based on the timing and completeness of each return.

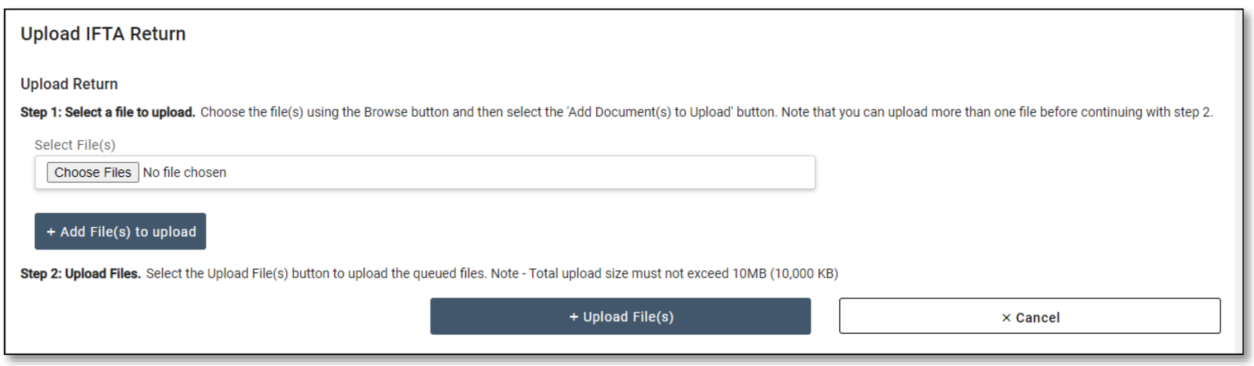


Figure 16: Upload IFTA Return

Core IFTA filing processes include:

- Original Returns
- Amended Returns
- Returns Appeal Process
- Reversals
- Audited Returns
- Estimated Assessments (aka Jeopardy Assessments)

All returns can be viewed at any time from any status. Return Statuses are:

- In Progress
  - Return is open to any changes and tax calculations that are allowed to be made for that return type.
- Filed (Not Paid)

    - The return is locked down and no changes can be made to it.
    - The official invoice is generated when the license, decal order or return is filed.
    - The invoice is available to be paid.
- Paid (Active)
    - For new or renewed licenses and additional decal orders, decals can be assigned either through a standard security task or automatically by the system via a scheduled batch job.
    - For IFTA returns, the "Paid (Active)" status indicates that the return is complete and will not be subject to the delinquency process.

Late Filing Interest

Returns submitted after the quarterly due date are considered late and may incur late filing interest charges. The MCC system automatically calculates and applies late filing interest at the time the return is filed.

To determine whether a return qualifies as late, MCC compares the quarter's due date with the return's postmark date. The postmark date can be backdated by authorized users on the return maintenance page. If no postmark date is provided, the system defaults to using the return's filed date. For online filers, the system uses the electronic file date to assess interest and penalties.

Late filing interest is calculated in accordance with Section R1230 of the IFTA Articles of Agreement, ensuring compliance with established regulatory standards.

Late Filing Penalty

Returns filed after the quarterly due date are considered late and may incur a Late Filing Penalty, which is calculated and charged at the time the return is filed.

For quarterly filers, if the return's postmark or filed date is after the due date, it is subject to a late filing penalty.

Amended Returns – Penalty Assessment Options

The MCC system provides three options for jurisdictions to determine whether an amended return is eligible for a late filing penalty. Jurisdictions must select one of the following:

Option 1: Based on Amendment Filing Date

- Each amendment is evaluated independently of the original return.
- If the amendment is filed after the due date, it is eligible for a penalty.
- The system does not consider whether the original return's penalty was waived.
- Users with appropriate permissions must manually waive penalties if needed.

Option 2: Based on Original Filing Date (Penalty Status Ignored)

- The system evaluates the original return's postmark/filed date.

Internal

- If the original return was late, the amendment is eligible for a penalty—regardless of whether the original penalty was waived.
  - Late + Penalty Not Waived → Amendment eligible
  - Late + Penalty Waived → Amendment still eligible
  - On Time → Amendment not eligible

Option 3: Based on Original Filing Date (Penalty Must Be Charged)

- The system checks if a penalty was actually charged on the original return.
- Amendment is eligible only if:
  - The original return was late and
  - A penalty was charged (amount > $0)
  - If the original penalty was waived (amount = $0), the amendment is not eligible.

IFTA Financial Processing

The MCC Financial Subsystem manages a wide range of financial functions, including payments, batches, account credits, and fund balances. It provides robust Payment Processing capabilities that allow taxpayers to make secure online payments, while staff can process payments received over the counter or by mail. To streamline the payment experience, MCC supports consolidated payments, enabling multiple invoices to be paid simultaneously with a single transaction. The system integrates seamlessly with the base jurisdiction's payment portal or credit card swipe device through Explore's custom interface, ensuring a smooth and user-friendly experience. MCC is highly configurable to support base jurisdiction-specific financial rules, including options to apply payments at either the Account or Invoice level. Additionally, jurisdictions can implement Pay in Order rules to prioritize the application of payments toward tax, interest, and penalties in a defined sequence.

When a jurisdiction has exhausted all reasonable efforts to collect the full amount due on an invoice, MCC allows the invoice to be marked as uncollectable. This designation triggers the system to retrieve the pro-rated uncollectable portion from previously transmitted IFTA Clearinghouse funds. The uncollectable function is used only after all collection avenues have been thoroughly pursued by the jurisdiction, ensuring proper financial reconciliation and adherence to IFTA procedures.

Internal

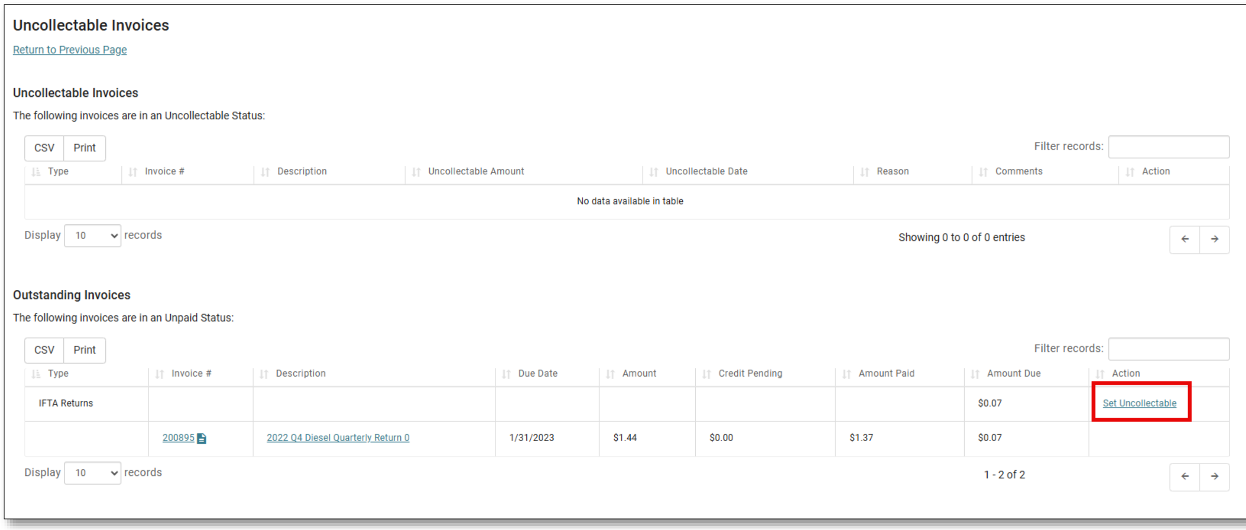


Figure 17: Uncollectable Invoices Utility

All fees, such as tax, interest, and penalty, within MCC are mapped to the base jurisdiction's designated account revenue stream fund. The system allows one or more fees to be mapped to the same fund and also supports splitting individual fees across multiple funds. Fee splitting is handled during invoice generation, while the invoice is presented to the customer as a unified total. The MCC Finance subsystem tracks payments at both the fee and fund levels to support detailed financial reporting. MCC transmits IFTA payments and refunds to the base jurisdiction's financial system through a custom interface, tailored to meet jurisdiction-specific requirements.

MCC supports a variety of payment methods, including cash, check, and external payment systems, which can be configured to align with the base jurisdiction's specific requirements. The system allows invoice payments to be split across multiple payment methods, offering flexibility for both taxpayers and staff. Payment types within MCC are categorized as either certified or non-certified. When an account is flagged for non-sufficient funds (NSF), MCC automatically enforces restrictions by disallowing non-certified payment methods and requiring certified funds for all future transactions. In such cases, clear messaging is displayed on both the Account Dashboard and associated invoices to notify the customer of the certified payment requirement. These controls ensure compliance with financial policies and support accurate, secure payment processing.

Internal

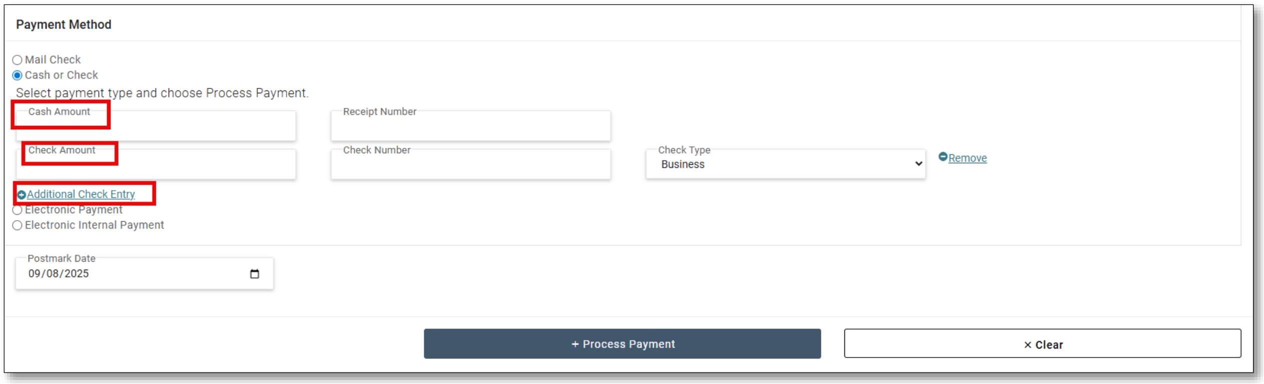


Figure 18: Split Payment Methods Example

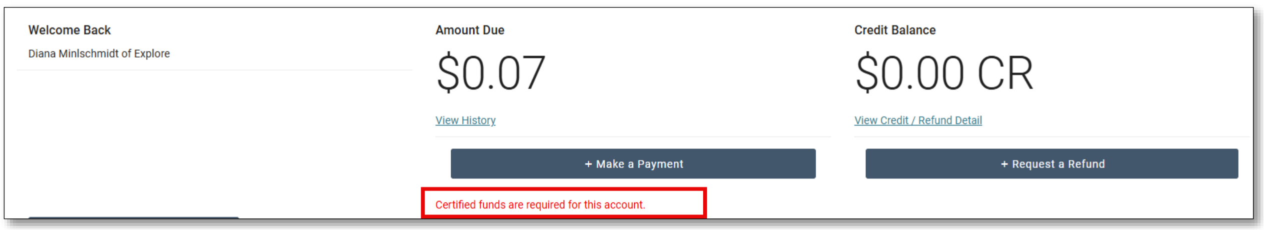


Figure 19: Certified Funds Required Message on Account Dashboard

Finance Credit Management

MCC provides comprehensive credit management capabilities for IFTA Returns and IFTA Orders (Decals), supporting multiple credit types that are maintained outside of the IFTA tax calculation process. These credits are generated and applied after returns have been filed and invoices have been generated. They are distinct from credits calculated during the IFTA return process, such as those resulting from amended filings or reversals, which are based on return details and jurisdictional rules.

The following finance credit types are maintained within MCC for IFTA:

- **Escrow Credit:** Generated when an invoice is marked as unpaid after the daily financial batch has been closed. Applicable to both IFTA Returns and Decal Orders.
- **Overpayment Credit:** Created when a payment exceeds the invoiced amount. Maintained for both IFTA Returns and Decal Orders.
- **Deposit Credit:** Manually added or withdrawn by authorized users as financial adjustments.
- **IFTA Return Credit:** Automatically generated when a return or amendment is filed or reversed, and a credit is calculated based on the return details.
- **IFTA Filing Write-Off Credit:** Generated when an IFTA Return invoice is written off. This credit is configurable and can be applied based on predefined thresholds set by the jurisdiction. If the jurisdiction elects to write off small balances or credits, MCC will

Internal

generate a credit equal to the write-off amount and apply it to the invoice to bring the balance to zero.

- **Custom Credit Types:** New credit types can be added as needed to meet the requirements of the base jurisdiction.

MCC credit management provides the following:

- Maintaining finance credits at the account or fleet level
- Automatically reserving applicable credits when an application is filed and the invoice is generated
- Applying credits to specific invoices
- Managing credit refund requests
- Removing reserved credits from invoices when necessary

When IFTA returns are filed, MCC automatically generates invoices and, for jurisdictions that have enabled the auto-reserve credit feature, the system evaluates available account credits to apply toward the invoice. MCC follows a configurable credit hierarchy to determine which credits to reserve first. For example, the system may be set to prioritize overpayment credits, followed by escrow credits, then deposit credits, and finally IFTA Return credits. This structured approach ensures that available credits are applied efficiently and in accordance with jurisdictional preferences during the filing process.

Finance Exceptions

MCC provides flexible exception handling for IFTA financial transactions, allowing authorized users to manage payment removals under two distinct scenarios:

- **After the Payment Has Been Deposited**
  If a payment has already been deposited into the base jurisdiction's financial system but needs to be removed, MCC enables authorized users to perform this action in accordance with jurisdiction-specific financial procedures. Once removed, the payment amount is converted into escrow credit and made available for future use.

- **Before the Payment Is Deposited**
  If a payment is still in process and has not yet been deposited, it can be voided based on the finance batch status. In this scenario, no credit is applied to the account, ensuring that only finalized payments impact account balances.

In both cases, MCC can transmit the payment removal details to the base jurisdiction's financial system through a custom interface and records a complete audit trail. This ensures transparency, accountability, and alignment with jurisdictional financial policies. The audit trail captures all relevant transaction details, supporting compliance and enabling thorough tracking for financial reviews and audits.

Internal

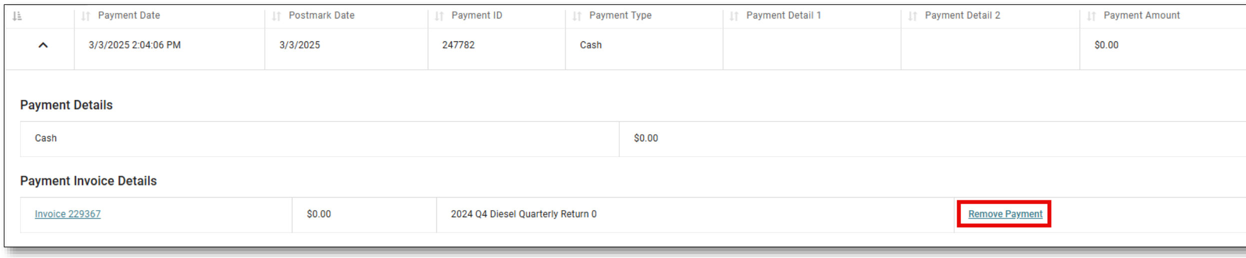


Figure 20: Remove IFTA License Payment Option

Finance Utilities

Adjust Invoice

Each fee within MCC, whether associated with IRP applications, IFTA decals, IFTA returns, permits, or other invoice types, can be configured to be adjustable based on the base jurisdiction's requirements. For any fee eligible for adjustment, MCC allows the jurisdiction to define specific adjustment reasons and require supporting comments. This high level of configurability ensures that fee adjustments are consistent with jurisdictional policies and business rules. Every adjustment transaction is fully audited, with a detailed audit trail maintained to support transparency, accountability, and regulatory compliance.

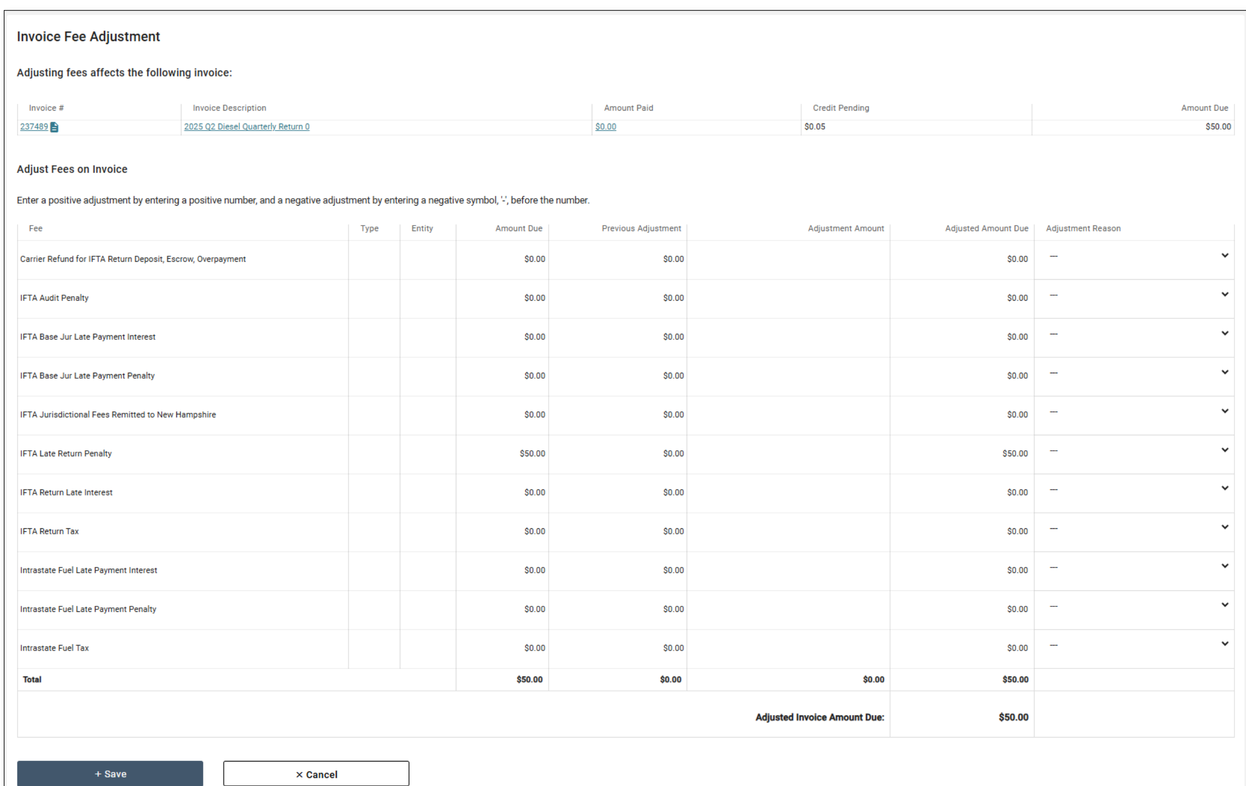
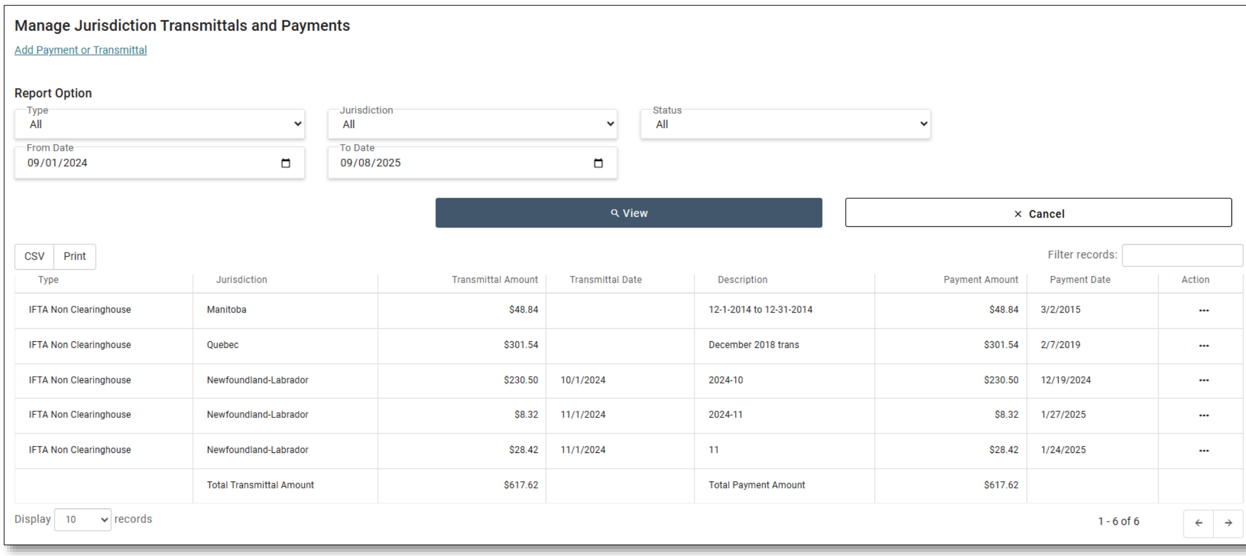


Figure 21: Adjust Invoice

Internal

Manage Jurisdiction Payments

The MCC system includes a configurable utility for managing jurisdictional transmittal payments applicable to both IFTA and IRP programs. This utility supports the base jurisdiction in reconciling payments owed by non-participating clearinghouse members or received through the IFTA Clearinghouse's monthly netting process. It is designed to accommodate jurisdiction-specific preferences and can be tailored to align with the base jurisdiction's financial policies. As a shared utility across both IFTA and IRP, it ensures consistent, accurate, and efficient handling of jurisdictional payment obligations.



Type	Jurisdiction	Transmittal Amount	Transmittal Date	Description	Payment Amount	Payment Date	Action
IFTA Non Clearinghouse	Manitoba	$48.84		12-1-2014 to 12-31-2014	$48.84	3/2/2015	...
IFTA Non Clearinghouse	Quebec	$301.54		December 2018 trans	$301.54	2/7/2019	...
IFTA Non Clearinghouse	Newfoundland-Labrador	$230.50	10/1/2024	2024-10	$230.50	12/19/2024	...
IFTA Non Clearinghouse	Newfoundland-Labrador	$8.32	11/1/2024	2024-11	$8.32	1/27/2025	...
IFTA Non Clearinghouse	Newfoundland-Labrador	$28.42	11/1/2024	11	$28.42	1/24/2025	...
	Total Transmittal Amount	$617.62		Total Payment Amount	$617.62		

Figure 22: Manage Jurisdiction Transmittal and Payments Utility

Manage Funds

The MCC system maintains fund balances for the base jurisdiction to support accurate financial reporting and reconciliation activities. Authorized users can manually adjust fund balances using a dedicated utility that ensures all updates are controlled, auditable, and traceable. This utility provides the flexibility needed to manage fund allocations in accordance with jurisdiction-specific financial policies, while maintaining a comprehensive audit trail to promote transparency, accountability, and compliance.

Quick Pay

A Quick Pay utility is provided to state users with authority to be able to process multiple payments across multiple accounts from a single web page versus accessing each carrier's account. The payments can be applied at the account level or the invoice level. For accounts that have unpaid invoices, and the account payment level is selected, the system will apply pay in order rules across finance systems to process the payment. Payments made through this utility can also be passed on to the base jurisdiction's financial system.

Processing NSF Transactions

If a payment is submitted but fails to clear, MCC allows the transaction to be marked as NSF (Non-Sufficient Funds). This automatically flags the account based on the base jurisdiction's restriction settings and sets the "Required Certified Funds?" indicator to "Yes", enforcing the use of certified payment methods. Additionally, the system supports a configurable "Require Certified Funds Through Date", which can be set to enforce certified funds for a defined period, such as a specific number of months, years, or indefinitely, based on the base jurisdiction's policies. MCC also creates an account-level restriction tied directly to the NSF Redemption transaction. Once the associated invoice is paid in full, the system automatically removes the restriction, restoring the account's normal payment status.

Credentials Administration

Motor Carrier Connect (MCC) provides secure, role-based credential management through its web-based application, supporting the full lifecycle of IRP and IFTA credential issuance, replacement, and inventory tracking.

MCC refers to "Tags" as Plates within the system and supports a comprehensive set of credential management functions tailored to Oklahoma's jurisdictional needs:

Plate Management

- **Request Replacement for Lost, Stolen, or Damaged Plates**
  Registrants can initiate plate replacement requests directly from their account dashboard. The workflow is streamlined to support quick resolution and credential reissuance.
- **Produce Plate Inventory**
  MCC includes a robust Inventory Management Subsystem that tracks plate inventory across multiple office locations. Inventory can be viewed, reported, and managed in real time, supporting both automatic and manual assignment methods.
- **Assign Plate Inventory to Registrants**
  Authorized users can assign plate inventory using either automated FIFO rules or manual selection of specific plate numbers, ensuring accurate tracking and assignment.

Cab Card Management

- **Reprint Cab Cards**
  Authorized users can reprint cab cards through the MCC interface, subject to security permissions and jurisdictional configuration. Reprints are logged for audit and compliance purposes, and may be restricted if the base jurisdiction requires reissuance through a formal application process.

Internal

- **Modify Cab Card Information**
  MCC supports real-time modification of cab card data through supplement workflows. Updated credentials can be issued immediately upon approval.

- **Issue Temporary Cab Cards**
  MCC allows for the issuance of temporary cab cards with configurable expiration periods.

- **QR Code Integration for Credential Verification**
  Cab cards can include QR codes that link directly to the MCC system for secure, real-time credential verification by enforcement officers.

- **Jurisdiction-Specific Messaging**
  The base jurisdiction can maintain and update custom messaging on cab cards using the User Maintained Text utility. This feature allows independent updates without requiring support from Explore.

- **Cab Card Control Number**
  Each cab card is assigned a unique control number, which supports direct search and retrieval of the associated unit within MCC. This control number is also used in law enforcement interfaces to verify the validity of the cab card and registration in real time, enhancing roadside enforcement and compliance.

IFTA Decal Management

MCC supports comprehensive IFTA decal administration, including:

- **Request Replacement Decals**
  Licensees can request replacements for damaged decals directly through the MCC interface.

- **Request Additional Decals**
  During renewals and decal requests, licensees may request up to 25% more decals than their fleet size. This validation rule is configurable and will be set on the base jurisdiction’s specific requirements.

- **Decal Inventory Reporting**
  MCC includes robust reporting capabilities for decal inventory. Licensees can generate account-level reports showing all decals issued by registration year. Administrators have access to detailed inventory views, including available, assigned, issued, and pending decals.

- **Security and Compliance Controls**
  All decal-related actions are governed by role-based permissions and license status. Only accounts in good standing are permitted to request additional decals. MCC enforces these conditions through configurable validation rules and automated compliance checks.

Internal

Control and Audit Features

All credentials, including plates, cab cards, and decals, are assigned unique control numbers to support tracking, audit readiness, and compliance. MCC's credential workflows are designed to ensure secure issuance, minimize manual intervention, and maintain full visibility across all credentialing activities.

Required Materials Management

The Motor Carrier Connect (MCC) system includes a configurable Required Materials module designed to ensure that all necessary documentation is collected before an application can proceed. This module dynamically determines which documents are required based on specific actions taken during the application process, such as adding units, initiating a new business, or requesting plate replacements.

Required documents can be configured for both IRP and/or IFTA workflows, allowing jurisdictions to enforce documentation requirements across both programs. MCC supports core configuration options that allow jurisdictions to define rules and triggers for required materials. These rules can be tailored to reflect both system-driven logic and jurisdiction-specific requirements.

Each document type can be configured with its own workflow stopping point, meaning the system will prevent the carrier from advancing until the required documentation is submitted, reviewed, and approved by staff.

Key capabilities include:

- **Dynamic Document Requirements**: Automatically identifies required documents based on application activity.
- **Jurisdiction-Specific Configuration**: Allows states to define additional required documents based on their own policies.
- **Workflow Enforcement**: Each document is assigned a stopping point in the workflow, ensuring that incomplete applications cannot proceed.
- **PDF Reporting**: MCC generates a comprehensive PDF report listing all outstanding documents required for the application and/or specific vehicles, supporting both carrier visibility and administrative review.

This module enhances compliance, streamlines document collection, and ensures that applications are complete before submission or approval.

Internal

Permitting

Motor Carrier Connect (MCC) features a fully integrated and configurable Permit Management System that supports the issuance, tracking, and reporting of multiple permit types, including IRP Trip Permits, IFTA Fuel Permits, and Unladen (Hunter's) Permits. The system is designed to meet the base jurisdictional requirements while providing a streamlined experience for both internal staff and external users.

Permit requests can be initiated directly from a dedicated link on the MCC login page, allowing carriers to apply for permits without needing a login ID. This public-facing portal supports secure access and payment processing, enabling quick and efficient permit issuance.

Each permit type is configurable, with support for jurisdiction-defined fields, validations, and expiration logic. MCC generates permits in standard 8.5x11 format, displaying critical information such as effective and expiration dates/times, vehicle details, and jurisdiction-specific messaging. The expiration rules are fully configurable to align with Oklahoma's regulatory standards.

Key capabilities include:

- **IRP Trip Permits**: Carriers and service providers can create, file, pay for, and track trip permits directly through MCC's public-facing portal, accessible from the login page without requiring a user ID. Internal users access the permit module from within the MCC system, using the Permit Maintenance interface to manage and monitor permit activity. All permit actions, whether initiated externally or internally, are logged and fully reportable, supporting transparency, compliance, and operational oversight.
- **IFTA Fuel Permits**: MCC supports creation and management of fuel permits with validations for vehicle weight and jurisdictional travel. Both internal and external workflows are supported.
- **Unladen (Hunter's) Permits**: MCC enables full lifecycle management of unladen permits, including creation, payment, and tracking, using the same workflow structure as other permit types.

All permit-related actions are governed by role-based security and are fully reportable within MCC. The system ensures consistency, compliance, and operational efficiency across all permit types.

Audit Management

The MCC Audit Management module is a fundamental component of the system and is designed to provide jurisdictions with a robust, configurable, and secure environment for managing all aspects of IFTA and IRP audits in accordance with the IRP Audit Procedures Manual and IFTA Audit Manual. The system supports the entire audit lifecycle, from account selection and audit initiation to review, appeal, and closure.

The audit process begins with the ability to group audits, allowing for joint IFTA and IRP audits and the sharing of high-level information across related cases. MCC's inheritance feature ensures that information entered at the group level is automatically applied to individual audits, while still allowing authorized users to break inheritance and customize audits as needed.

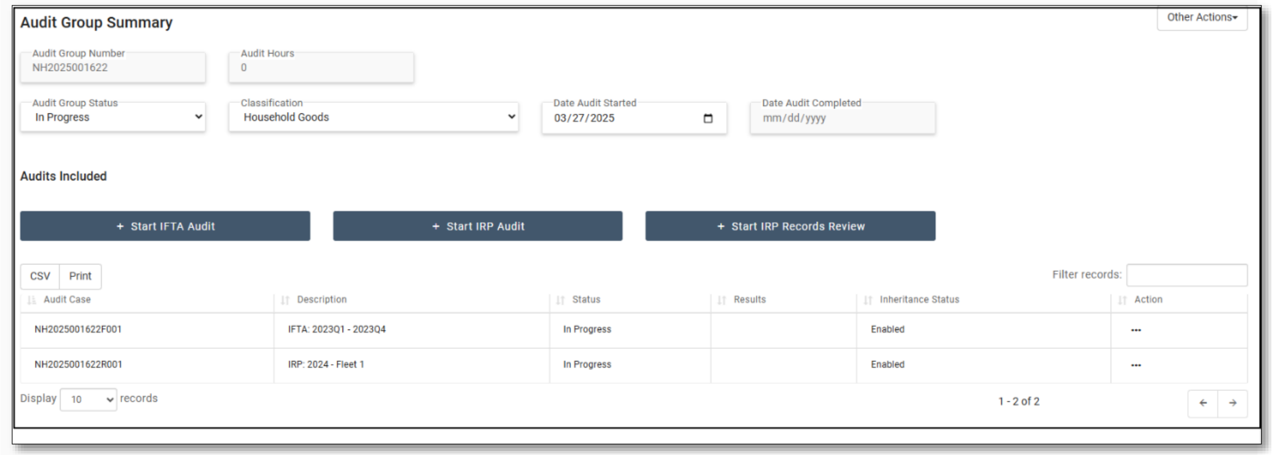


Figure 23: Audit Group Summary

Audits progress through a series of well-defined statuses, such as In Progress, Requesting Review, Review in Progress, Review Completed, In Appeal Period, In Protest, and Complete. Each status transition is governed by user security roles and jurisdictional business rules, ensuring that only authorized personnel can advance audits through the workflow. Automated email notifications keep audit teams and reviewers informed at key stages, such as when an audit is ready for review or when the review is complete.

MCC provides robust audit support tools for both IFTA and IRP programs, enabling jurisdictions to efficiently identify and manage audit candidates. For IFTA, MCC generates a stratification report that ranks all IFTA accounts into high, medium, and low strata based on IFTA requirements. This report includes demographic information, a summary of distance, jurisdiction count, and previous audit history to support informed audit selection.

For IRP, MCC offers an audit selection report that helps auditors identify eligible fleets based on actual miles reported during the selected registration period. The report includes a count of jurisdictions where actual miles were reported, and a count of units registered during the specified timeframe as well as IRP audit history of the account.

The base jurisdiction can use both stratification and account selection reports to prioritize audits, focusing on accounts flagged for audit or those with specific restrictions. MCC also allows users to maintain detailed audit contacts and logs, supporting transparent communication between audit teams and carriers. This comprehensive audit functionality promotes accountability, improves audit planning, and aligns with jurisdictional compliance strategies.

Audit creation and editing within MCC are streamlined through group-level data entry, which is inherited by individual audits unless inheritance is intentionally disabled. MCC also maintains

Internal

detailed audit notes and text fields for each audit, supporting comprehensive recordkeeping and transparency throughout the audit process.

MCC allows current year audits for both IFTA and IRP. During the IFTA audit period, MCC locks tax returns to prevent amendments, ensuring the integrity of the audit process. Auditors can manually enter, or upload amended returns and schedules, with built-in validations to ensure compliance with jurisdictional rules. The system calculates taxes, interest, and penalties based on audited information, applying rules specific to each jurisdiction. Audit invoices are generated automatically and can be adjusted by authorized users as needed.

During the IRP audit period, MCC allows users to submit supplements for the registration period being audited unless an audit supplement has already been initiated and is actively in progress. Once an audit supplement is started, the system restricts further supplement submissions to preserve the integrity of the audit data. After the audit enters the appeal period, MCC reopens the ability to submit supplements for the audited registration period. Once the appeal period concludes, the system evaluates any changes to reported miles or active units. If modifications are detected, MCC automatically triggers a fee recalculation and places the audit back into the appeal period to ensure accurate financial and compliance outcomes.

MCC provides a suite of standard and customizable reports, including Interjurisdictional Reports, Auditor Summary Reports, and Excel data downloads for further analysis. These reporting tools enable jurisdictions to analyze audit outcomes, compare reported and audited data across jurisdictions, and maintain transparency throughout the audit process. MCC generates an annual activity report for both IFTA and IRP for the bas jurisdiction to easily report audit outcomes for IRP and IFTA compliance. The system also supports appeal and protest workflows, allowing audits to enter an appeal period upon completion and supporting the management of protested audits, reversals, and related cases.

If an audit is reversed, MCC maintains the original audit case to preserve data integrity. The reversal is linked directly to the original audit, making it easy to reference and ensuring that a complete historical record of the audit process is available for compliance and audit trail requirements.

Furthermore, MCC tracks user assignments to active audits. The system notifies administrators when user accounts are inactivated, ensuring that audits are properly reassigned and continuity is maintained.

Records Reviews

Motor Carrier Connect (MCC) supports the administration of Records Reviews for both IRP and IFTA accounts. These reviews are designed to assess account accuracy and compliance without resulting in additional fees, taxes, or penalties. Unlike formal audits, Records Reviews serve as a proactive compliance tool and are conducted in alignment with IRP and IFTA Audit Procedures Manuals.

Internal

Each Records Review tracks similar data points as a full audit, including account details, documentation, and a narrative summary. Upon completion, MCC generates a comprehensive summary report that can be used for internal review and jurisdictional reporting.

To support compliance tracking, MCC counts three Records Reviews as equivalent to one audit for reporting purposes. This ratio is reflected in the jurisdiction's annual IRP and IFTA audit reports, ensuring transparency and alignment with plan requirements.

Records Reviews are fully integrated into MCC's workflow and reporting modules, allowing jurisdictions to manage, document, and report these activities with the same efficiency and security as formal audits.

Security Administration / Configuration Management

The MCC system is designed with a highly dynamic security structure that enforces separation of duties to mitigate risks associated with incompatible roles within the system. This approach ensures that sensitive operations are distributed among different users, thereby enhancing security and accountability. In MCC, security tasks are defined to control what users can do or see within the system. These tasks are assigned to one or more security roles, which are then mapped to user accounts. This mapping allows for granular control over access and functionality, ensuring that no single user possesses excessive privileges that could lead to unauthorized actions or data breaches.

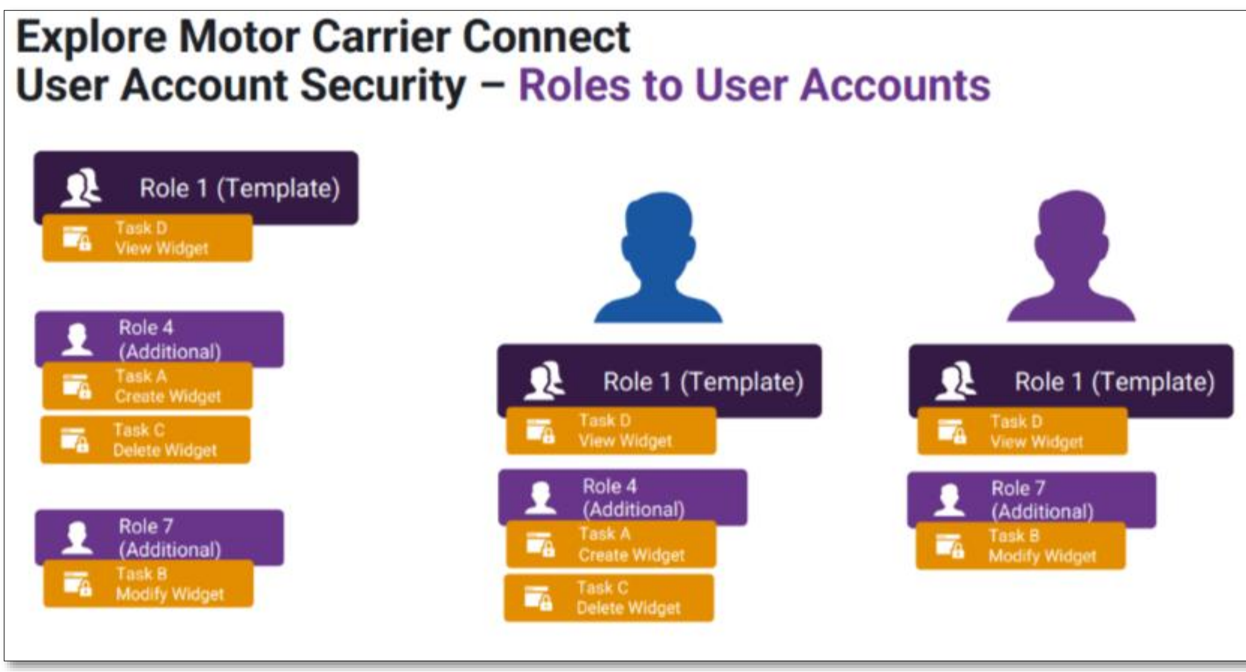


Figure 24: MCC User Roles to User Accounts

Internal

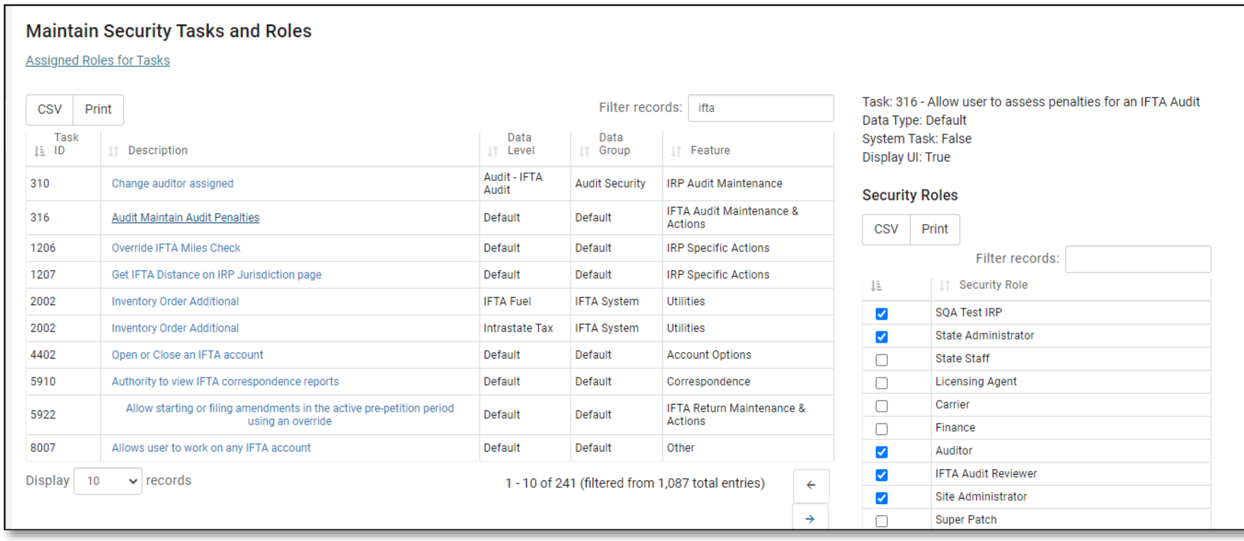


Figure 25: Security Role Maintenance Utility

The configuration and determination of security roles are managed by the base jurisdiction's state administrators. The intent is to create distinct roles that enforce the principle of separation of duties. This structure helps to minimize the risk of conflicts of interest by ensuring that users have access only to the functions necessary for their job responsibilities

State administrators utilize a specialized utility to determine which security tasks belong to each role. This tool aids in the systematic assignment of tasks to roles, ensuring clarity and compliance with established security policies

User accounts are assigned one or more roles based on their job functions, and administrators are responsible for maintaining these assignments. Administrators have the authority to change the roles assigned to user accounts as needed, facilitating flexibility while still adhering to security protocols.

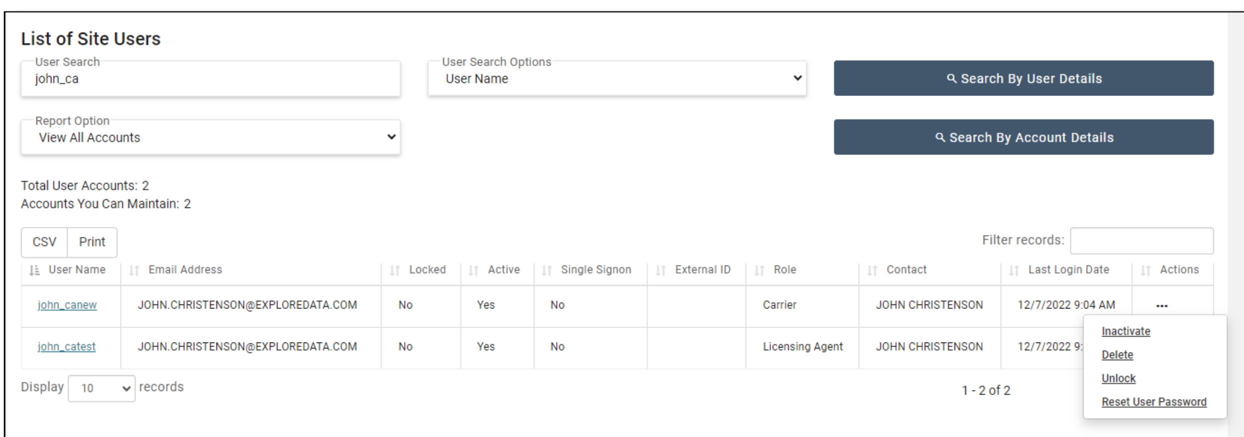


Figure 26: Maintain User Accounts Utility

Internal

To ensure transparency and accountability, the MCC system maintains a comprehensive audit trail that logs tasks associated with each role and tracks the roles assigned to user accounts. This audit trail allows for ongoing monitoring and review of user activities, helping to identify any potential security issues or violations of the separation of duties principle.

Inventory Management

The MCC Inventory Subsystem plays a crucial role in managing inventory status and tracking IRP plates, year decals, and IFTA decals. It provides a comprehensive solution for effectively managing and monitoring inventory within the system.

The system offers automated assignment of inventory based on user-specified locations. When inventory needs to be assigned, the system can automatically select and allocate the appropriate inventory from the specified location. Alternatively, manual assignment is also supported, giving users the flexibility to manually assign inventory as needed.

MCC accommodates multiple office locations and allows for the tracking of inventory at various locations within those offices. This feature enables jurisdictions with multiple offices to efficiently manage their inventory across different physical locations.

Authorized state users have the ability to add new inventory locations and deactivate existing ones as necessary. This functionality ensures that the system remains up-to-date and accurately reflects the current inventory status.

In addition to managing inventory within the base jurisdiction’s own offices, MCC also supports consignment inventory. This feature allows the jurisdiction to provide inventory to third-party entities that are approved by the jurisdiction for self-plating or issuance of decals. The system can facilitate the tracking and management of consignment inventory, ensuring accurate records and accountability.

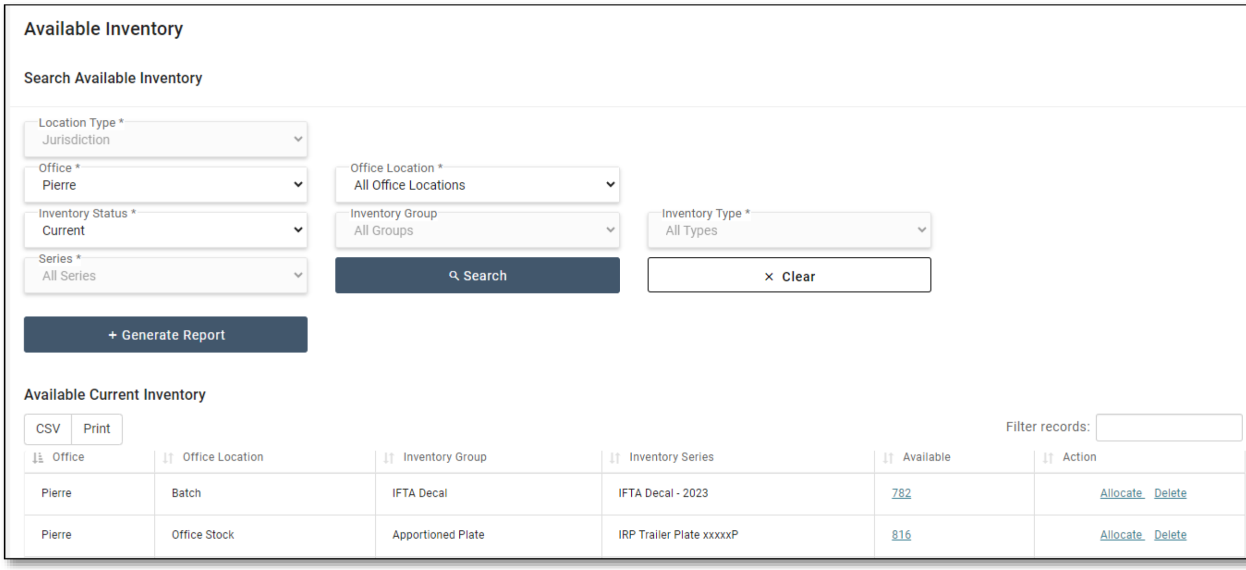


Figure 27: Maintain Inventory Utility

MCC provides multiple inventory assignment methods to accommodate operational needs and user security roles:

- **Assign Inventory Automatically**
    - When a user selects automatic assignment, the system determines which plate and decal inventory to use based on first-in, first-out (FIFO) rules. This ensures efficient inventory rotation and minimizes manual intervention.
- **Assign Inventory Manually**
    - Users with appropriate security permissions can manually enter plate numbers or decal serial numbers into the assignment page. The entered inventory items must exist in the Explore inventory system to be valid for assignment.
- **Batch Inventory Assignment (Overnight Processing)**
    - MCC also supports batch inventory assignment through an automated overnight job. This process assigns inventory to eligible applications and transactions based on jurisdictional configuration. As part of the batch job, MCC generates detailed reports listing all transactions that received inventory, along with corresponding packing slips. These reports support operational tracking, inventory reconciliation, and fulfillment workflows.

Internal

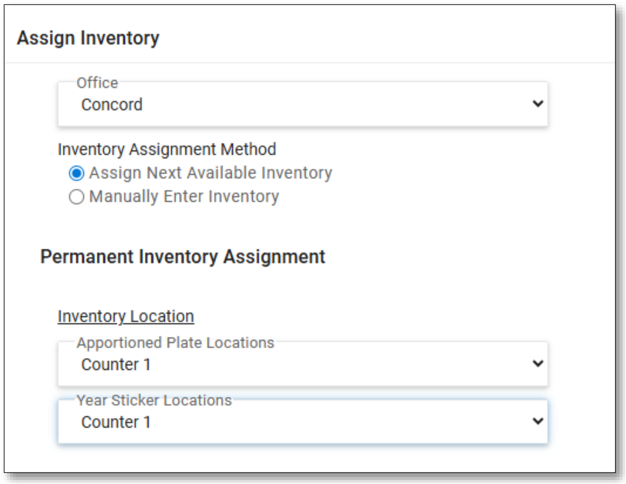


Figure 28: Assign Next Available Inventory on Receive Credentials Page

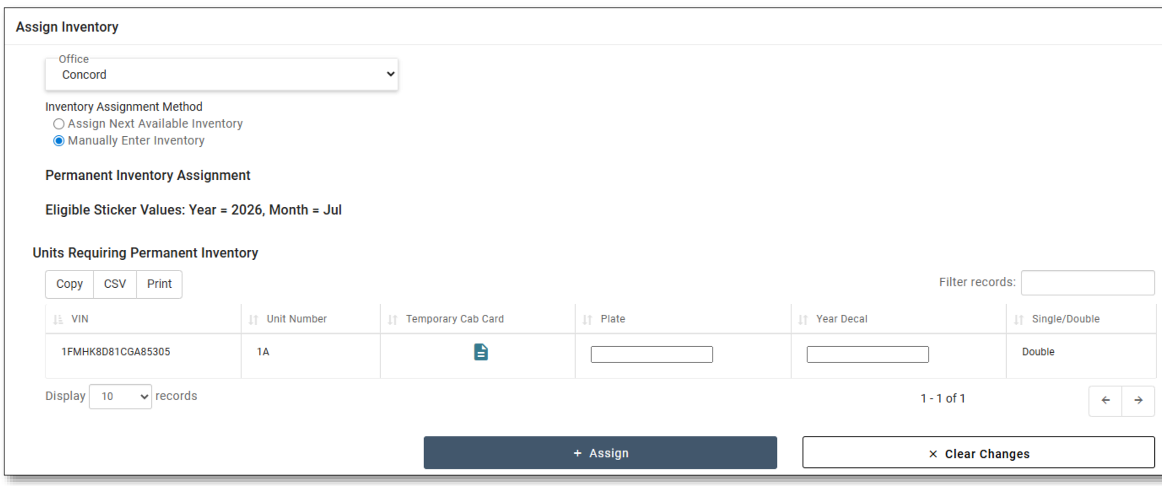


Figure 29: Manually Enter Inventory on Receive Credentials page

Document Management

The MCC system offers a comprehensive document management feature that enables users to upload documents to various entities such as accounts, applications, and audits. When a document is uploaded by a carrier or licensing agent, it enters a designated queue where state staff members can access and perform actions such as review, edit, approval, or denial, based on jurisdiction-specific requirements and policies. This review process ensures that all submitted documents meet the necessary criteria and comply with the base jurisdiction's standards.

To further support jurisdictional workflows, MCC can interface with the base jurisdiction's system of record to transmit and retrieve documents as needed. This integration facilitates seamless exchange of documentation between MCC and external systems, ensuring that all relevant materials are properly stored, accessible, and synchronized across platforms.

Internal

The document management feature in MCC provides a centralized and organized approach to handling documentation across accounts, applications, and audits. It supports efficient retrieval, tracking, and processing of uploaded documents, streamlining workflows for state staff responsible for review and approval. By enabling clear visibility into document status and history, MCC promotes transparency, accuracy, and compliance with jurisdictional standards. This functionality also fosters effective collaboration between state staff and carriers, ensuring that required documentation is properly submitted, reviewed, and managed within the system.

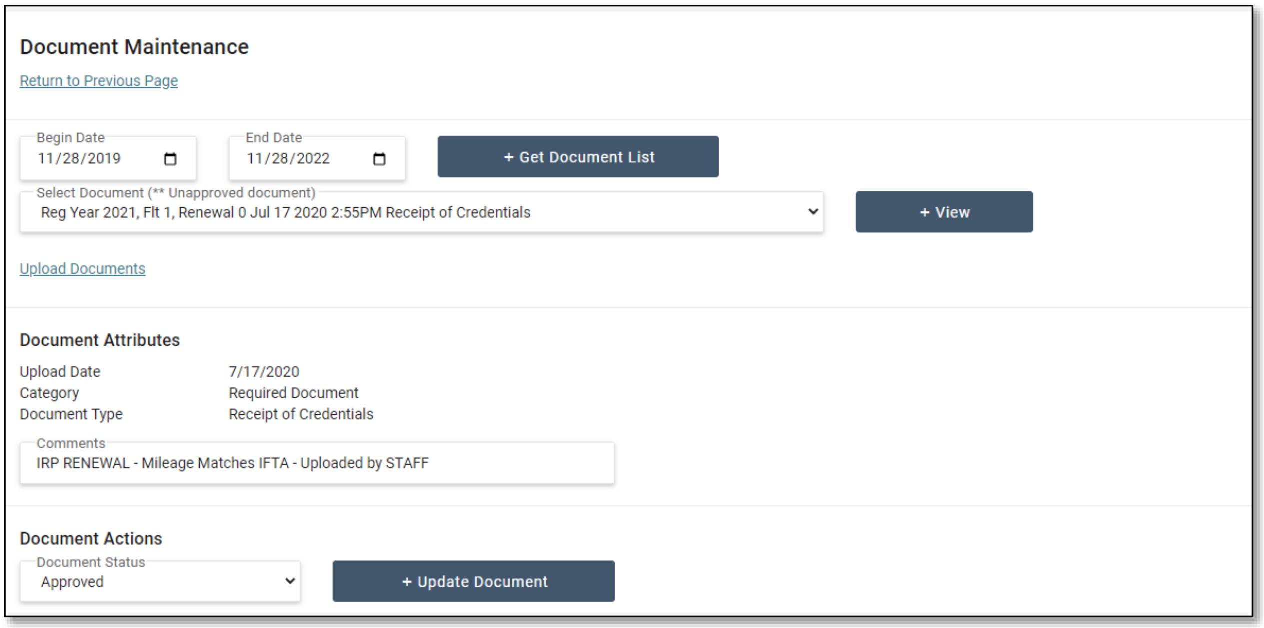


Figure 30: Maintain Documents Utility

In addition, MCC provides a Required Materials Needed widget on the Account Dashboard that notifies the carrier that outstanding documents are needed.

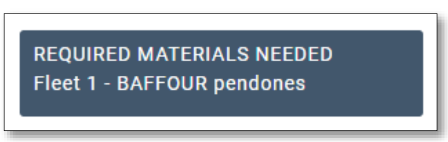


Figure 31: Required Materials Needed Widget

Communications / Correspondence Management

The MCC Communications Subsystem manages system generated correspondence and batch job output. MCC includes a utility for administrators to maintain user-defined text on forms, web pages and system generated e-mail messages. There is also a utility to maintain state office address information and tool to map office address information to forms, credentials and correspondence.

MCC can generate account level correspondence with user-created/maintained templates. Any correspondence that is generated for an account, including automated notifications, are available for authorized users to view at the account level.

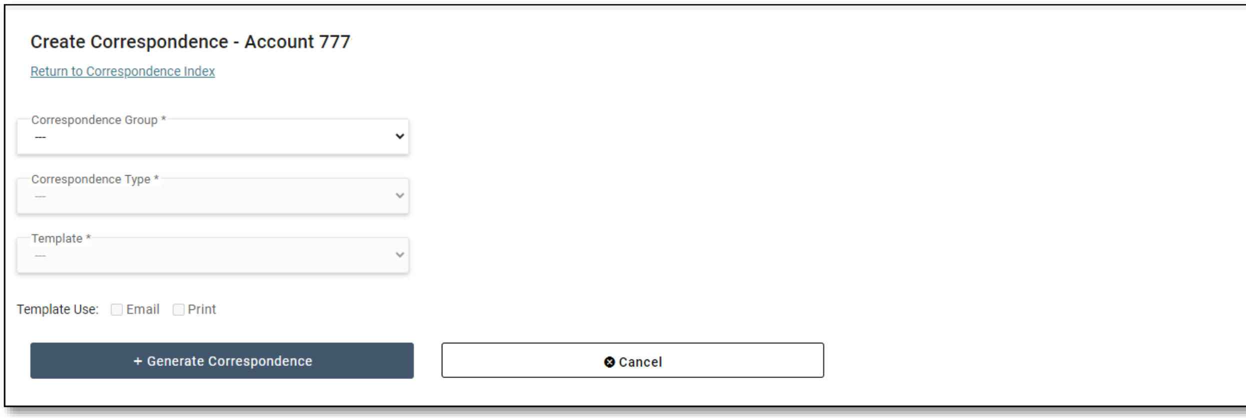


Figure 32: Create Account Correspondence Template

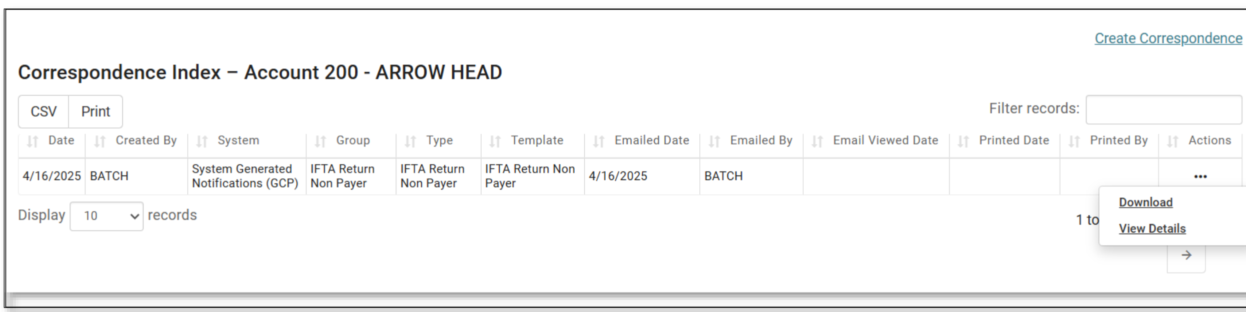
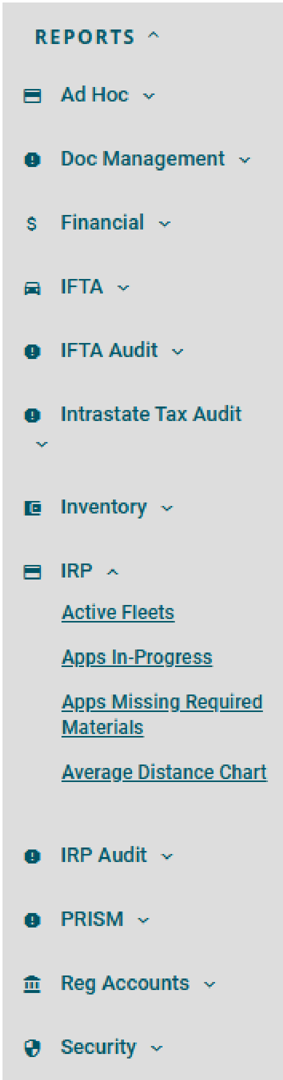


Figure 33: Account Correspondence

Reporting

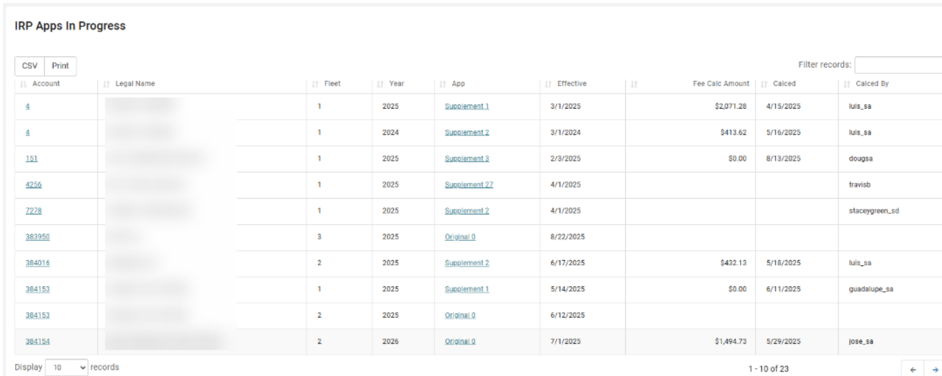
MCC provides an extensive suite of reporting tools, including standard canned reports, scheduled reports, and powerful ad-hoc reporting options. These reports support operational, compliance, and analytical needs across IRP, IFTA, Audits, Security, Inventory, Account Management, and more!

Internal



Canned Reports

Explore offers a wide variety of pre-built reports that cover core business functions. These reports are available in multiple formats including HTML, PDF, Microsoft® Excel®, and CSV. Each report includes a built-in dynamic filtering text box within the data grid. As users type into the filter, the system automatically narrows the displayed records to those containing matching text in any column, allowing for quick, intuitive refinement without needing to export or re-run the report.


IRP Apps In Progress

CSV Print Filter records:

Account	Legal Name	Fleet	Year	App	Effective	Fee Calc Amount	Calced	Calced By
4		1	2025	Supplement 1	3/1/2025	$2,071.28	4/15/2025	luis_sa
4		1	2024	Supplement 2	3/1/2024	$413.62	5/16/2025	luis_sa
151		1	2025	Supplement 3	2/3/2025	$0.00	8/13/2025	dougsa
4256		1	2025	Supplement 27	4/1/2025			travisb
7278		1	2025	Supplement 2	4/1/2025			staceygreen_sd
383950		3	2025	Original 0	8/22/2025			
384016		2	2025	Supplement 2	6/17/2025	$432.13	5/18/2025	luis_sa
384153		1	2025	Supplement 1	5/14/2025	$0.00	6/11/2025	guadalupe_sa
384153		2	2025	Original 0	6/12/2025			
384154		2	2026	Original 0	7/1/2025	$1,494.73	5/29/2025	jose_sa

Display 10 records 1 - 10 of 23

Figure 34 Sample Canned Report

Ad-Hoc Reporting

The ad-hoc reporting feature is highly flexible and virtually limitless in scope. Explore can create and deploy custom, nonstandard reports directly into production without code moves, making them immediately available for use. These reports can be re-run at any time and are downloadable in CSV format, providing ongoing access to critical data without requiring technical expertise or system downtime.

Self-Service Reporting

MCC includes Easy Query, a true self-service ad-hoc reporting tool that empowers users to create, save, share, search, and export customized reports independently. Users can build reports using intuitive filters and field selections, with output available in multiple formats including CSV for easy data manipulation.

All reporting features are governed by role-based security controls to ensure appropriate access and data protection. MCC's reporting framework supports transparency, operational oversight, and informed decision-making across all levels of jurisdictional operations.

IFTA Clearinghouse Interface

The MCC system automates the generation and transmission of IFTA data to the IFTA Clearinghouse, ensuring accurate and timely reporting without requiring user intervention. This

Internal

includes the monthly transmittal of IFTA financial data and the daily upload of IFTA demographics and decal files. MCC supports both Option 1 and Option 2 for transmitting IFTA return and audit data, as defined by the IFTA governing documents. As part of this automated process, MCC also produces jurisdiction-specific PDF reports for each transmittal period. These reports provide a clear summary of the data submitted to the Clearinghouse, supporting auditability, reconciliation, and compliance with IFTA reporting requirements.

IRP Clearinghouse Interface

Explore's Motor Carrier Connect (MCC) system successfully interfaces with IRP Inc.'s International Registration Plan Data Repository (IDR), enabling automated, secure, and standards-compliant data exchange. This integration ensures the timely and accurate transmission of registration data, including transmittals, recaps, and audit-related information, in accordance with IRP specifications.

The MCC system supports automated file transfers to the IRP Clearinghouse, including applicable IDR records, without requiring manual user intervention. Secure transmission protocols and validation mechanisms are built into the interface to maintain data integrity and compliance.

Explore has implemented this interface across multiple jurisdictions and maintains ongoing alignment with IRP Inc. standards through regular updates and coordination efforts. This robust integration streamlines jurisdictional reporting, enhances audit readiness, and reinforces MCC's role in supporting efficient and compliant motor carrier registration processes.

PRISM Compliance

Explore's Motor Carrier Connect (MCC) system is fully equipped to support PRISM (Performance and Registration Information Systems Management) compliance through a comprehensive set of automated features and interfaces. These capabilities ensure alignment with FMCSA requirements and facilitate accurate, timely data exchange with federal and state systems.

Key PRISM compliance functionalities include:

- **Live Interactive API:** Enables real-time data exchange and validation with PRISM-related systems.
- **Baseline Snapshots:** Automatically transmitted to state CVIEW systems or IRP Inc.'s IDR to support enforcement and monitoring.
- **US DOT/TIN Validations:** Ensures carrier identity verification and eligibility checks.
- **PRISM TARGET File Matching:** MCC prevents the issuance of credentials to carriers with VINs that are revoked or suspended by FMCSA or other jurisdictions.
- **Automated Correspondence:** System-generated notifications related to PRISM status and enforcement actions.

Internal

- **PRISM-Compliant Reporting:**
  - Dynamically generated PDF Cab Cards and Temporary Cab Cards with 2D barcodes conforming to PRISM specifications.
  - Daily SAFER-compliant transaction sets:
    - IDR1 (IRP Account), IDR2 (Fleet), and IDR3 (Unit), IDR4 (Baseline) records.
    - T0019 (IFTA)

These integrated features ensure MCC supports all aspects of PRISM compliance, helping jurisdictions enforce safety accountability and maintain accurate registration data across systems.

Internal

Section Eight: Pricing

Pricing for the Motor Carrier Connect (MCC) IRP/IFTA system is detailed in the accompanying Exhibit-02 Cost Sheet (refer to *Section 08-01-Exhibit_02_Cost_Sheet.pdf document)*. This document reflects all required pricing components, including one-time costs, customization, training, and renewal options. Our bid remains valid for a minimum of 120 days from the Bid Response Due Date, and all usage estimates provided by the State are understood to be non-binding.

The pricing structure is based on the following interpretation of the cost sheet: In the "Renewal Options" table, the Initial Cost is the sum of Table 1 ("One-Time Cost for IFTA/IRP application"), Table 2 ("Customizing the application," which includes data conversion), and Table 3 ("One-Time cost for on-site training"). The Total Cost in the Renewal Options table includes the Initial Cost plus the annual costs for Years 1 through 5. The Grand Total reflects the full cost of implementation and support over the initial five-year term. Therefore, the Total amount in the "Renewal Options" table is the same as the "Grand Total."

Internal

Exhibit 2 - Cost Sheet New IFTA/IRP System

Fields highlighted in yellow **shall** be used in calculating low price determination. Prospective Suppliers **shall not** alter the Cost Sheet.

Table 1 - Provide the total, one-time cost for IFTA/ IRP application

IFTA/ IRP application already built and utilized by other agencies.	
One Time Cost	$ $450,000

Table 2 - Provide the total hours and cost for customizing the application to meet the needs of the Oklahoma Corporation Commission.

Customizing	
Hourly Cost	$ Hours: 2750 Total Cost $400,000

Table 3 - Provide the total, one-time cost for on-site or online training [if applicable]

Training	
One Time Cost	$ $50,000

Renewal Options						
Initial Cost	Year 1	Year 2	Year 3	Year 4	Year 5	Total
$ 900,000	$ 450,000	$ 375,000	$ 375,000	$ 375,000	$ 375,000	$ 2,850,000

Table 4

Grand Total
$ **2,850,000**

NOTE:
Renewal Options Table:
Initial Cost = Sum of Tables 1, 2, and 3
Total Cost = Initial Cost plus Years 1 - 5

The **Grand Total** reflects the full cost of implementation and support over the initial five-year term. Therefore, the Total amount in the "Renewal Options" table is the same as the "Grand Total."

Section Nine: Offer of Value-Added Products and/or Services

Explore Information Services, LLC is not proposing any additional value-added products or services beyond those already included in our core solution. However, we are pleased to confirm that our proposed Motor Carrier Connect (MCC) system delivers a comprehensive suite of features and services at no additional cost to the State.

The MCC platform includes robust functionality such as:

- IRP and IFTA processing
- Trip and Fuel Permits
- Mobile-friendly, responsive design
- Document management
- Dynamic security task configuration
- Integrated audit tools
- Custom interfaces and data conversion
- Onsite training, UAT coordination, and post-implementation support

These capabilities are fully integrated into the base solution and are provided as part of Explore's standard implementation and support services. Our approach ensures that the State receives a complete, modernized IRP/IFTA system without the need for optional add-ons or incremental pricing.

Explore's commitment is to deliver a full-featured solution that meets and exceeds the State's requirements, without hidden costs or fragmented offerings.

Internal