



STATE OF MICHIGAN ENTERPRISE PROCUREMENT

Department of Technology, Management, and Budget
320 S. Walnut Street 2nd Floor Lansing, MI 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number 5
to
Contract Number MA230000001706

CONTRACTOR	Information Services Corporation
	10 Research Drive Suite 300
	Regina SK
	Riley Meloche
	306-531-5318
	riley.meloche@isc.ca
	VS0296576

STATE	Program Manager	Various	Various
STATE	Contract Administrator	Jarrod Barron	
		517-249-0406	
		BarronJ1@michigan.gov	

CONTRACT SUMMARY				
Uniform Commercial Code (UCC) System				
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE	
November 1, 2023	November 1, 2028	5 - 12 Months	November 1, 2028	
PAYMENT TERMS		DELIVERY TIMEFRAME		
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
<input type="checkbox"/> P-Card <input type="checkbox"/> Direct Voucher (PRC) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
MINIMUM DELIVERY REQUIREMENTS				
DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>		
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$3,344,042.00	\$897.00	\$3,344,939.00		

DESCRIPTION

Effective 4/17/2025, the parties add \$897.00 for the services detailed in the attached Enhancement 42097 statement of work. All other terms, conditions, specifications and pricing remain the same. Per Contractor, agency, and DTMB Central Procurement approval.

Further, the parties add the following language to the Contract:

"Accessibility Requirements. The State is required to comply with the Americans with Disabilities Act of 1990 (ADA) and has adopted standards and procedures regarding accessibility requirements for websites, applications, content, and electronic documents. Due to a change in the law, the State is required to comply with specific accessibility standards for websites, applications, content and documents. Starting 4/24/2026, throughout the Term, all websites, applications, software, content, and electronic documents, including but not limited to mobile applications, text, images, sounds, videos, controls, animations, links, and documents (including files in the following formats: PDF, word processing, presentation, and spreadsheet), created, provided, or made available by the Contractor under this Contract, must comply with WCAG 2.1 Level AA."

Per Contractor, Agency, and DTMB Procurement approval. Internal State Note: Remaining Ad Board funds after this CN: \$181,060.99.

**Program Managers
for
Multi-Agency and Statewide Contracts**

AGENCY	NAME	PHONE	EMAIL
DTMB	Daniel Klodt	517-930-6368	KlodtD@michigan.gov
MDOS	Keitha Cameron	517-231-0152	CameronK1@michigan.gov

STATEMENT OF WORK - IT CHANGE NOTICE

Project Title: UNIFORM COMMERCIAL CODE (UCC) SYSTEM Enhancement 42097	Period of Coverage: 3/26/2025-11/1/2028
Requesting Department: Department of State (MDOS)	Date: March 25, 2025
Agency Project Manager: Rayne Sherman	Phone: 517-275-2862
DTMB Project Manager: Dan Klodt	Phone: 517-930-6368

BACKGROUND:

When a Subscription order is generated in the Michigan UCC system, a single PDF document is created and sent to the user. This PDF document includes multiple filing images, which are individually processed and then merged to form one document.

SCOPE OF WORK:

As described in the following DevOps Item: [ENHANCEMENT 42097](#)

Description:

Please provide an estimate of hours and cost to change the file format for the image subscription. Desired format would be for each image to be an individual PDF with the filing number as the file name. All individual PDFs would then need to be delivered in some sort of file together, not individual delivery.

ISC TASKS & DELIVERABLES:

Technical support is required to assist with the following tasks:

- *Development of requested change to split the subscription images.*
- *System Testing*
- *Deployment – Promotion of the changes to Development, UAT and Production environments.*

MDOS TASKS:

- *User Acceptance Testing*
- *Approval to promote to Production based on Testing*

ACCEPTANCE CRITERIA:

The development work completed will require testing to be completed by the designated Michigan UCC business tester(s). Testing sign-off will be provided once testing has been successfully

completed and the business is satisfied with the change. Testing will occur in the UAT environment and is tracked on the associated DevOps board. Deliverables will not be considered complete until the Agency Project Manager and DTMB Project Manager have formally accepted them.

PROJECT CONTROL AND REPORTS:

A bi-weekly progress report must be submitted to the Agency and DTMB Project Managers throughout the life of this project. This report may be submitted with the billing invoice. Each bi-weekly progress report must contain the following:

- **Accomplishments:** Indicate what was worked on and what was completed during the current reporting period.

SPECIFIC DEPARTMENT STANDARDS:

Agency standards, if any, in addition to DTMB standards.

PAYMENT SCHEDULE:

Payment will be made on a one-time fixed price. Contractor may invoice the State for \$897.00 after all deliverables have been fully tested and accepted by the Agency Project Manager and DTMB Project Manager.

EXPENSES:

The State will NOT pay for any travel expenses, including hotel, mileage, meals, parking, etc.

PROJECT CONTACTS:

The designated Agency Project Manager is:

Rayne Sherman
MDOS - Office of Business and Internal Services
SOS Secondary Complex – 1st Floor
7064 Crowner Drive
Dimondale, MI 48821
Phone: 517-275-2862
ShermanR@Michigan.gov

The designated DTMB Project Manager is:

Dan Klodt
DTMB - BRM
Austin Building 3rd Floor
430 W. Allegan St.
Lansing, MI 48933
517-930-6368
KlodtD@Michigan.gov

AGENCY RESPONSIBILITIES:

As agreed in **Contract Number 230000001706**.

LOCATION OF WHERE THE WORK IS TO BE PERFORMED:

Consultants will work at:

Regina, Saskatchewan, Canada

EXPECTED CONTRACTOR WORK HOURS AND CONDITIONS:

Work hours are not to exceed eight (8) hours a day, forty (40) hours a week. Normal working hours of 8:00 am to 5:00 pm are to be observed unless otherwise agreed to in writing.

No overtime will be permitted.



**STATE OF MICHIGAN
ENTERPRISE PROCUREMENT**

Department of Technology, Management, and Budget
320 S. Walnut Street 2nd Floor Lansing, MI 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **4**
to
Contract Number **MA230000001706**

CONTRACTOR	Information Services Corporation
	10 Research Drive Suite 300
	Riley Meloche
	306-531-5318
	riley.meloche@isc.ca
	VS0296576

STATE	Program Manager	Various	Various
STATE	Contract Administrator	Jarrod Barron	DTMB
		(517) 249-0406	
		BarronJ1@michigan.gov	

CONTRACT SUMMARY				
Uniform Commercial Code (UCC) System				
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE	
November 1, 2023	November 1, 2028	5 - 12 Months	November 1, 2028	
PAYMENT TERMS		DELIVERY TIMEFRAME		
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
<input type="checkbox"/> P-Card <input type="checkbox"/> Direct Voucher (PRC) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
MINIMUM DELIVERY REQUIREMENTS				
DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>		
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$3,344,042.00	\$0.00	\$3,344,042.00		
DESCRIPTION				
Effective 1/27/2025, the parties add the attached escrow agreement to the contract. All other terms, conditions, specifications, and pricing remain the same. Per contractor, agency, and DTMB Central Procurement approval.				
Internal State Note: Remaining Ad Board funds after this CN: \$181,957.99.				

**Program Managers
for
Multi-Agency and Statewide Contracts**

AGENCY	NAME	PHONE	EMAIL
DTMB	Daniel Klodt	517-930-6368	KlodtD@michigan.gov
MDOS	Keitha Cameron	517-231-0152	CameronK1@michigan.gov

Effective Date	
Deposit Account Number	
*Effective Date and Deposit Account Number to be supplied by NCC Group only.	

Three-Party Escrow Service Agreement

1. Introduction

This Three Party Escrow Service Agreement (the “**Agreement**”) is entered into by and between Information Services Corporation (the “**Depositor**”), and by the State of Michigan (the “**Beneficiary**”) and by NCC Group Software Resilience (NA) LLC (“**NCC Group**”), a Delaware limited liability company. Depositor, Beneficiary, and NCC Group may be referred to individually as a “**Party**” or collectively as the “**Parties**” throughout this Agreement.

- (a) The use of the term services in this Agreement shall refer to NCC Group services that facilitate the creation, management, and enforcement of software or other technology escrow accounts as described in Exhibit A attached to this Agreement (“**Services**”). A Party shall request Services under this Agreement by selecting such Service on Exhibit A upon execution of the Agreement or by submitting a work request for certain NCC Group Services (“**Work Request**”) via written instruction or websites owned or controlled by NCC Group (collectively the “**NCC Group Website**”).
- (b) The Beneficiary and Depositor have entered into Software Contract Terms and Conditions effective as of November 1, 2023 (“**License Agreement**”) conveying intellectual property rights to the Beneficiary, and the Parties intend this Agreement to be considered as supplementary to such agreement, pursuant to Title 11 United States [Bankruptcy] Code, Section 365(n).

2. Depositor Responsibilities and Representations

- (a) It shall be solely the Depositor’s responsibility to: (i) make an initial deposit of all proprietary technology and other materials covered under this Agreement (“**Deposit Material**”) to NCC Group within thirty (30) days of the Effective Date; (ii) make any required updates to the Deposit Material during the Term (as defined below) of this Agreement; and (iii) ensure that a minimum of one (1) copy of Deposit Material is deposited with NCC Group at all times. At the time of each deposit or update, Depositor will provide an accurate and complete description of all Deposit Material sent to NCC Group using the form attached to this Agreement as Exhibit B.
- (b) Depositor represents that it lawfully possesses all Deposit Material provided to NCC Group under this Agreement and that any current or future Deposit Material liens or encumbrances will not prohibit, limit, or alter the rights and obligations of NCC Group under this Agreement. Depositor warrants that with respect to the Deposit Material, NCC Group’s proper administration of this Agreement will not violate the rights of any third parties.
- (c) Depositor represents that all Deposit Material is readable and useable in its then current form; if any portion of such Deposit Material is encrypted, the necessary decryption tools and keys to read such material are deposited contemporaneously.

3. Beneficiary Responsibilities and Representations

- (a) Beneficiary acknowledges that, as between NCC Group and Beneficiary, NCC Group’s obligation is to maintain the Deposit Material as delivered by the Depositor and that, other than NCC Group’s inspection of the Deposit Material (as described in Section 4) and the performance of any of the optional verification Services listed in Exhibit A, NCC Group has no other obligation regarding the completeness, accuracy, or functionality of the Deposit Material.
- (b) It shall be solely the Beneficiary’s responsibility to monitor whether a deposit or deposit update has been accepted by NCC Group.

4. NCC Group Responsibilities and Representations

- (a) NCC Group agrees to use commercially reasonable efforts to provide the Services requested by Authorized Person(s) (as identified in the “**Authorized Person(s)/Notices Table**” below) representing the Depositor or Beneficiary in a Work Request. NCC Group may reject a Work Request (in whole or in part) that does not contain all required information at any time upon notification to the Party originating the Work Request.
- (b) NCC Group will conduct a visual inspection upon receipt of any Deposit Material and associated Exhibit B. If NCC Group determines that the Deposit Material does not match the description provided by Depositor represented in Exhibit B, NCC Group will notify Depositor of such discrepancy.
- (c) NCC Group will provide notice to the Beneficiary of all Deposit Material that is accepted and deposited into the escrow account under this Agreement. Either Depositor or Beneficiary may obtain information regarding deposits or deposit updates upon request or through the NCC Group Website.
- (d) NCC Group will follow the provisions of Exhibit C attached to this Agreement in administering the release of Deposit Material.

- (e) NCC Group will hold and protect Deposit Material in physical or electronic vaults within the United States that are either owned or under the control of NCC Group, unless otherwise agreed to by the Parties.
- (f) Upon receipt of written instructions by both Depositor and Beneficiary, NCC Group will permit the replacement or removal of previously submitted Deposit Material. The Party making such request shall be responsible for getting the other Party to approve the joint instructions. Any Deposit Material that is removed from the deposit account will be either returned to Depositor or destroyed in accordance with Depositor's written instructions.
- (g) Should transport of Deposit Material be necessary for NCC Group to perform Services requested by Depositor or Beneficiary under this Agreement or following the termination of this Agreement, NCC Group will use a commercially recognized overnight carrier such as Federal Express or United Parcel Service. NCC Group will not be responsible for any loss or destruction of, or damage to, such Deposit Material while in the custody of the common carrier.

5. Deposit Material Verification

- (a) Beneficiary may submit a verification Work Request to NCC Group for one or more of the Services defined in Exhibit A attached to this Agreement and Depositor consents to NCC Group's performance of any level(s) of such Services. Upon request by NCC Group and in support of Beneficiary's request for verification Services, Depositor shall promptly complete and return an escrow deposit questionnaire and reasonably cooperate with NCC Group by providing reasonable access to its technical personnel whenever reasonably necessary.
- (b) The Parties consent to NCC Group's use of a subcontractor to perform verification Services. Such subcontractor shall be bound by the same confidentiality obligations as NCC Group and shall not be a direct competitor to either Depositor or Beneficiary. NCC Group shall be responsible for the delivery of Services of any such subcontractor as if NCC Group had performed the Services. Depositor warrants and Beneficiary warrants, individually, that any material it supplies for verification Services is lawful, does not violate the rights of any third parties and is provided with all rights necessary for NCC Group to perform verification of the Deposit Material.
- (c) NCC Group will work with a Party who submits any verification Work Request for Deposit Material covered under this Agreement to either fulfill any standard verification Services Work Request or develop a custom Statement of Work ("**SOW**"). NCC Group and the requesting Party will mutually agree in writing to an SOW on terms and conditions that include but are not limited to: description of Deposit Material to be tested; description of verification testing; requesting Party responsibilities; NCC Group responsibilities; Service Fees; invoice payment instructions; designation of the paying Party; designation of authorized SOW representatives for both the requesting Party and NCC Group with name and contact information; and description of any final deliverables prior to the start of any fulfillment activity. Provided that the requesting Party has identified in the verification Work Request or SOW that the Deposit Material is subject to the regulations of the International Traffic in Arms Regulations (22 CFR 120)(hereinafter "**ITAR**"), NCC Group shall ensure that any subcontractor who is granted access to the Deposit Material for the performance of verification Services shall be a U.S. Person as defined in 8 U.S.C. 1101(a)(20) or who is a protected person as defined in 8 U.S.C. 1324b(a)(3). After the start of fulfillment activity, each SOW may only be amended or modified in writing with the mutual agreement of both Parties, in accordance with the change control procedures set forth in the SOW. If the verification Services extend beyond those described in Exhibit A, the Depositor shall be a necessary Party to the SOW governing the Services.

6. Payment

The Party responsible for payment designated in the Paying Party Billing Contact Table ("**Paying Party**") shall pay to NCC Group all fees as set forth in the Work Request ("**Service Fees**"). All Service Fees are due within thirty (30) calendar days from the date of invoice in U.S. currency and are non-refundable. NCC Group may update Service Fees with a ninety (90) calendar day written notice to the Paying Party during the Term of this Agreement (as defined below). The Paying Party is liable for any taxes (other than NCC Group income taxes) related to Services purchased under this Agreement or shall present to NCC Group an exemption certificate acceptable to the taxing authorities. Applicable taxes shall be billed as a separate item on the invoice. Any Service Fees not collected by NCC Group when due shall bear interest until paid at a rate of one percent (1%) per month (12% per annum) or the maximum rate permitted by law, whichever is less. Notwithstanding the non-performance of any obligations of Depositor to deliver Deposit Material under the License Agreement or this Agreement, NCC Group is entitled to be paid all Service Fees that accrue during the Term of this Agreement.

7. Term and Termination

- (a) The term of this Agreement is for a period of one (1) year from the Effective Date ("**Initial Term**") and will automatically renew for additional one (1) year terms ("**Renewal Term**") (collectively the "**Term**"). This Agreement shall continue in full force and effect until one of the following events occur: (i) Depositor and Beneficiary provide NCC Group with sixty (60) days' prior written joint notice of their intent to terminate this Agreement; (ii) Beneficiary provides NCC Group and Depositor with sixty (60) days' prior written notice of its intent to terminate this Agreement; (iii) the Agreement terminates under another provision of this Agreement; or (iv) any time after the Initial Term, NCC Group provides sixty (60) days' prior written notice to the Depositor and Beneficiary of NCC Group's intent to terminate this Agreement. The Effective Date and the Deposit Account Number shall be supplied by NCC Group only. The Effective Date supplied by NCC Group and specified above shall be the date NCC Group sets up the escrow account.

- (b) Unless the express terms of this Agreement provide otherwise, upon termination of this Agreement, NCC Group shall return physical Deposit Material to the Depositor and erase electronically submitted Deposit Material. If reasonable attempts to return the physical Deposit Material to Depositor are unsuccessful, NCC Group shall destroy the Deposit Material.
- (c) In the event of the nonpayment of undisputed Service Fees owed to NCC Group, NCC Group shall provide all Parties to this Agreement with written notice of NCC Group's intent to terminate this Agreement. Any Party to this Agreement shall have the right to make the payment to NCC Group to cure the default. If the past due payment is not received in full by NCC Group within thirty (30) calendar days of the date of such written notice, then NCC Group shall have the right to terminate this Agreement at any time thereafter by sending written notice to all Parties. NCC Group shall have no obligation to perform the Services under this Agreement (except those obligations that survive termination of this Agreement, which includes the confidentiality obligations in Section 10) so long as any undisputed Service Fees due NCC Group under this Agreement remain unpaid.

8. Infringement Indemnification

Anything in this Agreement to the contrary notwithstanding, Depositor at its own expense shall defend, indemnify and hold NCC Group fully harmless against any claim or action asserted against NCC Group (specifically including costs and reasonable attorneys' fees associated with any such claim or action) to the extent such claim or action is based on an assertion that NCC Group's administration of this Agreement infringes any patent, copyright, license or other proprietary right of any third party. When NCC Group has notice of a claim or action, it shall promptly notify Depositor in writing. Depositor may elect to control the defense of such claim or action or enter into a settlement agreement, provided that no such settlement or defense shall include any admission or implication of wrongdoing on the part of NCC Group without NCC Group's prior written consent, which consent shall not be unreasonably delayed or withheld. NCC Group shall have the right to employ separate counsel and participate in the defense of any claim at its own expense.

9. Warranties

NCC GROUP WARRANTS ANY AND ALL SERVICES PROVIDED HEREUNDER SHALL BE PERFORMED IN A COMMERCIALY REASONABLE MANNER CONSISTENT WITH INDUSTRY STANDARDS. EXCEPT AS SPECIFIED IN THIS SECTION, ALL CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW. AN AGGRIEVED PARTY MUST NOTIFY NCC GROUP PROMPTLY UPON LEARNING OF ANY CLAIMED BREACH OF ANY WARRANTY AND, TO THE EXTENT ALLOWED BY APPLICABLE LAW, SUCH PARTY'S REMEDY FOR BREACH OF THIS WARRANTY SHALL BE SUBJECT TO THE LIMITATION OF LIABILITY AND CONSEQUENTIAL DAMAGES WAIVER IN THIS AGREEMENT. THIS DISCLAIMER AND EXCLUSION SHALL APPLY EVEN IF THE EXPRESS WARRANTY AND LIMITED REMEDY SET FORTH ABOVE FAILS OF ITS ESSENTIAL PURPOSE.

10. Confidential Information

NCC Group shall have the obligation to implement and maintain safeguards designed to protect the confidentiality of the Deposit Material and use at least the same degree of care to safeguard the confidentiality of the Deposit Material as it uses to protect its own confidential information, but in no event less than a reasonable degree of care. Except as provided in this Agreement NCC Group shall not use or disclose the Deposit Material. NCC Group shall not disclose the terms of this Agreement to any third party other than its financial, technical, or legal advisors, or its administrative support service providers. Any such third party shall be bound by the same confidentiality obligations as NCC Group. If NCC Group receives a subpoena or any other order from a court or other judicial tribunal pertaining to the disclosure or release of the Deposit Material, NCC Group will promptly notify the Parties to this Agreement unless prohibited by law. After notifying the Parties, NCC Group may comply in good faith with such order or subpoena. It shall be the responsibility of Depositor or Beneficiary to challenge any such order or subpoena; provided, however, that NCC Group does not waive its rights to present its position with respect to any such order or subpoena. NCC Group will cooperate with the Depositor or Beneficiary, as applicable, to support efforts to quash or limit any order or subpoena, at such Party's expense.

11. Limitation of Liability

EXCEPT FOR: (I) LIABILITY FOR DEATH OR BODILY INJURY; (II) PROVEN GROSS NEGLIGENCE OR WILLFUL MISCONDUCT; OR (III) THE INFRINGEMENT INDEMNIFICATION OBLIGATIONS OF SECTION 8, ALL OTHER LIABILITY RELATED TO THIS AGREEMENT, IF ANY, WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, OF ANY PARTY TO THIS AGREEMENT SHALL BE LIMITED TO \$250,000 (USD).

12. Consequential Damages Waiver

IN NO EVENT SHALL ANY PARTY TO THIS AGREEMENT BE LIABLE FOR ANY INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, LOST PROFITS, ANY COSTS OR EXPENSES FOR THE PROCUREMENT OF SUBSTITUTE SERVICES (EXCLUDING SUBSTITUTE ESCROW SERVICES), OR ANY OTHER INDIRECT DAMAGES, WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE EVEN IF THE POSSIBILITY THEREOF MAY BE KNOWN IN ADVANCE TO ONE OR MORE PARTIES.

13. General

- (a) Purchase Orders. In the event that the Paying Party issues a purchase order or other instrument used to pay Service Fees to NCC Group, any terms and conditions set forth in the purchase order which constitute terms and conditions which are in addition to those set forth in this Agreement or which establish conflicting terms and conditions to those set forth in this Agreement are expressly rejected by NCC Group.
- (b) Right to Make Copies. NCC Group shall have the right to make copies of all Deposit Material as reasonably necessary to perform the Services. NCC Group shall copy all copyright, nondisclosure, and other proprietary notices and titles contained on Deposit Material onto any copies made by NCC Group. Any copying expenses incurred by NCC Group as a result of a Work Request to copy will be borne by the requesting Party. NCC Group may request Depositor's reasonable cooperation in promptly copying Deposit Material in order for NCC Group to perform this Agreement.
- (c) Choice of Law. The validity, interpretation, and performance of this Agreement shall be construed under the laws of the State of Michigan, USA, without giving effect to the principles of conflicts of laws.
- (d) Authorized Person(s). Depositor and Beneficiary must each authorize and designate one person whose actions will legally bind such Party ("**Authorized Person**" who shall be identified in the Authorized Person(s) Notices Table of this Agreement or such Party's legal representative) and who may manage the NCC Group escrow account through the NCC Group website or written instruction. Depositor and Beneficiary warrant that they shall maintain the accuracy of the name and contact information of their respective designated Authorized Person during the Term of this Agreement by providing NCC Group with a written request to update its records for the Party's respective Authorized Person which includes the updated information and applicable deposit account number(s).
- (e) Right to Rely on Instructions. With respect to release of Deposit Material or the destruction of Deposit Material, NCC Group shall rely on instructions from a Party's Authorized Person. In all other cases, NCC Group may act in reliance upon any instruction, instrument, or signature reasonably believed by NCC Group to be genuine and from an Authorized Person, officer, or other employee of a Party. NCC Group may assume that such representative of a Party to this Agreement who gives any written notice, request, or instruction has the authority to do so. NCC Group will not be required to inquire into the truth of, or evaluate the merit of, any statement or representation contained in any notice or document reasonably believed to be from such representative.
- (f) Force Majeure. No Party shall be liable for any delay or failure in performance due to events outside the defaulting Party's reasonable control, including without limitation acts of God, strikes, riots, war, acts of terrorism, fire, declaration of emergency by a federal, state or local authority, or delays of common carriers or other circumstances beyond its reasonable control. The obligations and rights of the excused Party shall be extended on a day-to-day basis for the time period equal to the period of the excusable delay.
- (g) Notices. NCC Group shall have the right to rely on the last known address provided by each the Depositor and Beneficiary for its respective Authorized Person and Billing Contact as set forth in this Agreement or as subsequently provided as an update to such address. All notices regarding Exhibit C (Release of Deposit Material) shall be sent by commercial express mail or other commercially appropriate means that provide prompt delivery and require proof of delivery. All other correspondence, including but not limited to invoices and payments, may be sent electronically or by regular mail. The Parties shall have the right to rely on the last known address of the other Parties. Any correctly addressed notice to the last known address of the other Parties, that is refused, unclaimed, or undeliverable shall be deemed effective as of the first date that said notice was refused, unclaimed, or deemed undeliverable by electronic mail, the postal authorities, or commercial express mail.
- (h) No Waiver. No waiver of any right under this Agreement by any Party shall constitute a subsequent waiver of that or any other right under this Agreement.
- (i) Assignment. No assignment of this Agreement by Depositor or Beneficiary or any rights or obligations of Depositor or Beneficiary under this Agreement is permitted without the written consent of NCC Group, which shall not be unreasonably withheld or delayed. Notwithstanding the foregoing, Beneficiary, in its sole discretion, may assign in whole or in part, its rights or responsibilities under this Agreement to any other governmental entity if such assignment is made reasonably necessary by operation of controlling law or regulation. NCC Group shall have no obligation in performing this Agreement to recognize any successor or assign of Depositor or Beneficiary unless NCC Group receives clear, authoritative and conclusive written evidence of the change of Parties.
- (j) Severability. In the event any of the terms of this Agreement become or are declared to be illegal or otherwise unenforceable by any court of competent jurisdiction, such term(s) shall be null and void and shall be deemed deleted from this Agreement. All remaining terms of this Agreement shall remain in full force and effect.
- (k) Independent Contractor Relationship. Depositor and Beneficiary understand, acknowledge, and agree that NCC Group's relationship with Depositor and Beneficiary will be that of an independent contractor and that nothing in this Agreement is intended to or should be construed to create a partnership, joint venture, or employment relationship.
- (l) Attorneys' Fees. Any costs and fees incurred by NCC Group in the performance of obligations imposed upon NCC Group solely by virtue of its role as escrow service provider including, without limitation, compliance with subpoenas, court orders, discovery requests, and disputes arising solely between Depositor and Beneficiary, including, but not limited to, disputes concerning a release of the Deposit Material shall, unless adjudged otherwise, be paid by Depositor.

- (m) No Agency. No Party has the right or authority to, and shall not, assume or create any obligation of any nature whatsoever on behalf of the other Parties or bind the other Parties in any respect whatsoever.
- (n) Disputes. The Parties agree that any dispute arising under this Agreement will be resolved in the state court of claims in Lansing, Michigan, and the parties hereby expressly consent to the jurisdiction thereof. EACH PARTY ACKNOWLEDGES AND AGREES THAT ANY CONTROVERSY THAT MAY ARISE UNDER THIS AGREEMENT IS LIKELY TO INVOLVE COMPLICATED AND DIFFICULT ISSUES AND, THEREFORE, EACH SUCH PARTY IRREVOCABLY AND UNCONDITIONALLY WAIVES ANY RIGHT IT MAY HAVE TO A TRIAL BY JURY IN RESPECT OF ANY LEGAL ACTION ARISING OUT OF OR RELATING TO THIS AGREEMENT.
- (o) Interpleader. Anything to the contrary notwithstanding, in the event of any dispute regarding the interpretation of this Agreement, or the rights and obligations with respect to the Deposit Material in escrow or the propriety of any action contemplated by NCC Group hereunder, then NCC Group may, in its sole discretion, file an interpleader or similar action in any court of competent jurisdiction to resolve any such dispute.
- (p) Regulations. Depositor and Beneficiary each represent and covenant that upon the Effective Date of this Agreement and throughout the term of this Agreement, that: (i) it is not identified on any restricted party lists; or located in countries identified on any restricted country lists; or using the Deposit Material or the Services for any restricted end uses; including those promulgated by the U.S. Departments of State, Commerce and Treasury; (ii) it is and shall remain compliant with all laws and regulations applicable to its performance under this Agreement, including, but not limited to ITAR, any export control and economic sanctions or government regulations of any country from or to which the Deposit Material may be delivered in accordance with the provisions of this Agreement; and (iii) it will not take any action that will cause NCC Group to be in violation of such laws and regulations, and will not require NCC Group to directly or indirectly take any action that might cause it to be in violation of such laws and regulations. Depositor will not provide NCC Group with Deposit Material that is subject to export controls and controlled at a level other than EAR99/AT. With respect to Deposit Material containing personal information and data, Depositor agrees to (i) procure all necessary consents in relation to personal information and data; and (ii) otherwise comply with all applicable privacy and data protection laws as they relate to the subject matter of this Agreement. NCC Group is responsible for and warrants, to the extent of their individual actions or omissions, compliance with all applicable laws, rules and regulations to the extent that it is directly regulated by the law, rule or regulation and to the extent that it knows or has been advised that, as a result of this Agreement, its activities are subject to the law, rule or regulation.
- (q) No Third Party Rights. This Agreement is made solely for the benefit of the Parties to this Agreement and their respective permitted successors and assigns, and no other person or entity shall have or acquire any right by virtue of this Agreement unless otherwise agreed to by all of the Parties.
- (r) Entire Agreement. The Parties agree that this Agreement, which includes all attached Exhibits and all valid Work Requests and SOWs submitted by the Parties, is the complete agreement between the Parties concerning the subject matter of this Agreement and replaces any prior or contemporaneous oral or written communications between the Parties. There are no conditions, understandings, agreements, representations, or warranties, expressed or implied, which are not specified in this Agreement. Each of the Parties warrant that the execution, delivery, and performance of this Agreement has been duly authorized and signed by a person who meets statutory or other binding approval to sign on behalf of its organization as named in this Agreement. This Agreement may be modified only by mutual written agreement of all the Parties.
- (s) Counterparts. This Agreement may be executed electronically in accordance with applicable law or in any number of counterparts, each of which shall be an original, but all of which together shall constitute one instrument.
- (t) Survival. Sections 7 (Term and Termination), 8 (Infringement Indemnification), 9 (Warranties), 10 (Confidential Information), 11 (Limitation of Liability), 12 (Consequential Damages Waiver), and 13 (General) of this Agreement shall survive termination of this Agreement or any Exhibit attached to this Agreement.


(BALANCE OF THIS PAGE LEFT INTENTIONALLY BLANK – SIGNATURE PAGE FOLLOWS)

IN WITNESS WHEREOF, the Parties have duly executed this Agreement as of the Effective Date by their authorized representatives:

DEPOSITOR		BENEFICIARY	
Signature		Signature	
Print Name	Loren Cisyk	Print Name	
Title	Executive Vice President, Technology Solutions	Title	
Date		Date	

NCC GROUP	
Signature	
Print Name	
Title	
Date	

**Approved as to Legal and Operational Content:
NCC Group**



**Name: Nikita Adatia, Contracts Attorney
Date: January 15, 2025**

(BALANCE OF THIS PAGE LEFT INTENTIONALLY BLANK – NOTICES TABLES AND EXHIBITS FOLLOW)

Authorized Person Notices Table			
Please provide the names and contact information of the Authorized Persons under this Agreement. Please complete all information as applicable. Incomplete information may result in a delay of processing.			
DEPOSITOR (Required information)		BENEFICIARY (Required information)	
Print Name	Loren Cisyk	Print Name	
Title	Executive Vice President, Technology Solutions	Title	
Email Address	Loren.Cisyk@isc.ca	Email Address	
Street Address	300 – 10 Research Drive	Street Address	
City	Regina	City	
State/Province	Saskatchewan	State/Province	
Postal/Zip Code	S4S 7J7	Postal/Zip Code	
Country	Canada	Country	
Phone Number		Phone Number	

Paying Party Billing Contact Information Table (Required information)	
Please provide the name and contact information of the Billing Contact for the Paying Party under this Agreement. All Invoices will be sent to this individual at the address set forth below. Incomplete information may result in a delay of processing.	
Company Name	Information Services Corporation
Print Name	Layne Rieger
Title	Procurement Manager
Email Address	Layne.Rieger@isc.ca
Street Address	300 – 10 Research Drive
City	Regina
State/Province	Saskatchewan
Postal/Zip Code	S4S 7J7
Country	Canada
Phone Number	
Purchase Order #	

NCC GROUP

All notices should be sent to SRclientservices@nccgroup.com OR NCC Group, Attn: Client Services, 6111 Live Oak Parkway, Norcross, Georgia, 30093, USA. Telephone: 800-875-5669.

Exhibit A
Escrow Services Fee Schedule – Work Request

Deposit Account Number

Service	Service Description - Three-Party Escrow Service Agreement All services are listed below. Check the requested service and submit a Work Request to NCC Group for services requested after agreement signature.	One-Time/Per Service Fees	Annual Fees
<input checked="" type="checkbox"/> Setup Fee (Required at Setup) <input checked="" type="checkbox"/> Deposit Account Fee (Required at Setup) <input checked="" type="checkbox"/> Beneficiary Fee (Required at Setup)	<p>One-time Setup Fee for NCC Group to setup a standard Three-Party Escrow Service Agreement.</p> <p>NCC Group will set up one deposit account to manage and administrate access to Deposit Material to be secured in a controlled storage environment. NCC Group will provide account services that include unlimited deposits, electronic vaulting, access to NCC Group Website for secure online account management, submission of electronic Work Requests, and communication of status. Release of deposit material is also included in the annual fee. An oversize fee of \$250 USD per 1.2 cubic foot will be charged for deposits that exceed 2.4 cubic feet.</p> <p>NCC Group will fulfill a Work Request to add a Beneficiary to an escrow deposit account and manage account access rights. Beneficiary will have access to NCC Group Website for secure online account management, submission of electronic Work Requests, and communication of status.</p>	\$3,215	\$1,400 \$1,065
<input type="checkbox"/> Media File Review Audit	<p>NCC Group will perform one (1) Media File Review Audit, which includes a Deposit Material media readability analysis, a file listing, a file classification table, virus scan outputs, and confirmation of the presence or absence of a completed escrow deposit questionnaire. A final report will be sent to the requesting Party regarding the Deposit Material. The deposit must be provided on CD, DVD-R, or deposited electronically.</p>	\$3,870	N/A
<input type="checkbox"/> Deposit Review Audit	<p>NCC Group will perform one (1) Deposit Review Audit on the specified deposit, which includes the outputs of the Media File Review, identifying the presence/absence of build, setup and design documentation (including the presence or absence of a completed escrow deposit questionnaire), and identifying materials required to recreate the Depositor's application development and production environments. Output includes a report that includes compile and setup documentation, file classification tables and file listings. The report will list required software development materials, including, without limitation, required source code languages and compilers, third-party software, libraries, operating systems, and hardware, and NCC Group's analysis of the deposit. A final report will be sent to the requesting Party regarding the Deposit Material.</p>	\$8,290 or based on SOW if custom work required	N/A
<input type="checkbox"/> Dual Vaulting	<p>NCC Group will store and manage a redundant copy of the Deposit Material in one (1) additional location. All Deposit Material (original and copy) must be provided by the Depositor.</p>	N/A	\$1,025
<input type="checkbox"/> Remote Vaulting	<p>NCC Group will store and manage the Deposit Material in a remote location, designated by the client, outside of NCC Group's primary escrow vaulting location. All Deposit Material (original and copy) must be provided by the Depositor.</p>	N/A	Call for Quote
<input type="checkbox"/> Custom Contract Fee	<p>Custom contract changes to NCC Group templates are subject to the Custom Contract Fee, which covers the review and processing of custom or modified contracts.</p>	\$1,575	N/A
<input checked="" type="checkbox"/> Entry Level Verification (ELV)	<p>NCC Group will perform an Entry Level Verification ("ELV") of source code and other material that Depositor will submit as Deposit Material. During the ELV, Depositor will demonstrate the completeness and functionality of the source code by compiling the code while being remotely observed online by an NCC Group Verification Consultant at a mutually agreeable time. The ELV consists of four phases. Phase One – the Verification Consultant reviews the requirements for the build including hardware and tools, examination of the structure and attributes of the source code and relevant associated files, which will be submitted as Deposit Material. Phase Two - the Depositor will compile the source code into a working application while under observation from the Verification Consultant. Phase Three – Depositor will verify that the build is successful and working as expected. The Verification Consultant will work with the Depositor to document the successful build and prepare an ELV report that will document the testing process and outcome. Phase four - Once testing is complete, Depositor shall submit the source code and files used for the ELV as Deposit Material. The Service Fee covers up to eight (8) hours over no more than two (2) consecutive business days.</p>	\$22,665	
<input type="checkbox"/> Independent Build Verification (IBV)	<p>Upon receipt of the Deposit Material, NCC Group will perform an Independent Build Verification ("IBV") of the source code. The IBV consists of the following steps: (1) prior to attempting the IBV, a review of the technical questionnaire (as submitted by the Depositor) or previous ELV report (if available) will be conducted by a technical NCC Group consultant; (2) the NCC Group consultant will prepare a suitable build environment, including configuring an appropriate operating system and installing the identified third party software required for compiling; (3) the Deposit Material will be transferred to the build environment. The NCC Group consultant will confirm if appropriate build documentation or instructions have been received; (4) The NCC Group consultant will attempt to build an executable version of the source code (following up as needed with the Depositor); (5) Upon a successful build, a copy of the executable version will be provided to the Beneficiary for testing; (6) The NCC Group consultant will process the deposit for storage and prepare an IBV report detailing the verification process and outcome.</p>	\$25,245	
General Terms for all tests and verifications	<p>Fees for testing are due in advance and testing will begin after payment of such fees. If through no fault of NCC Group, testing cannot be completed within twelve (12) months of being ordered, NCC Group will issue a final failed test report identifying the reason for the failure and the testing shall be considered completed. Prior to beginning testing, NCC Group will determine if third party tools or software are required for completion of testing. If such software or tools are required, NCC Group will bill the Paying Party at cost for the additional expense to acquire such tools or software. Testing will begin after payment of such expense. NCC Group reserves the right to cancel testing and issue a refund if NCC Group determines requirements for testing exceed its contemplated scope of testing services or if NCC Group determines it cannot provide such testing. Price is exclusive of expenses, VAT and sales tax. Verification Fees are subject to change in accordance with standard rates for services.</p>		

Additional Verification Services (Fees based on Statement of Work)	
Secure Verification (SAST)	NCC Group will perform a Static Application Security Test ("SAST") to identify any security vulnerabilities in the application source code. The SAST Verification consists of the following steps: (1) Scoping and review of questionnaire (as submitted by the Depositor), followed by an assessment of whether the code base provided is complete, and that all third party dependencies have been provided; (2) the NCC Group Consultant will work with the Depositor to resolve any compilation errors and obtain any missing assemblies or third party libraries; (3) where applicable, the NCC Group Consultant will conduct a pre-scan (translation) of the source code, to ensure the automated SAST assessment can be performed; (4) the NCC Group Consultant will perform an automated scan of the code to analyze the source code for security vulnerabilities. This will be performed using a Static Code Analyzer, (5) Upon completion of the SAST assessment, two reports will be produced. A technical report, containing all SAST assessment results and a list of all identified vulnerabilities will be issued to the Depositor. An executive summary report will be issued to the Beneficiary SAST analysis is available for the following languages: ABAP/BSP, ActionScript/MXML, ASP.NET, VB.NET, C# (.NET), C/C++, Classic ASP, COBOL, ColdFusion CFML, HTML, Java, JavaScript/AJAX, JSP, Objective-C, PHP, PL/ SQL, Python, T-SQL, Ruby, Swift, Visual Basic, VBScript, XML. Additional languages may be supported if agreed in writing between the parties after consultation and review of requirements.
Binary Comparison Verification	NCC Group will fulfill a Statement of Work (SOW) to perform one Binary Comparison Test - Binary Comparison, which includes the outputs of the IBV test, a comparison of the executable files built from the IBV Test to the actual executable files in use by the Beneficiary to ensure a full binary-level match, with a final report sent to the Requesting Party regarding the Deposit Material. The Paying Party and NCC Group will agree on a custom SOW prior to the start of fulfillment. A completed escrow deposit questionnaire is required for execution of this test.
Full Usability Verification	NCC Group will fulfill a Statement of Work (SOW) to perform one Deposit Usability Test - Full Usability, which includes which includes the outputs of the Deposit Review and IBV (if applicable). NCC Group will confirm that the deposited application can be setup, installed and configured and, when installed, will execute functional tests, based on pre-determined test scripts provided by the Parties, and create comprehensive setup and installation documentation. A final report will be sent to the Paying Party regarding the Deposit Material. The Paying Party and NCC Group will agree on a custom SOW prior to the start of fulfillment. A completed escrow deposit questionnaire is required for execution of this test.

Pursuant to the Agreement, the undersigned hereby issues this Work Request for performance of the Service(s) selected above.

Paying Party – For Future Work Request Use Only	
Paying Party Name	
Signature	
Print Name	
Title	
Date	

NCC GROUP

All Work Requests should be sent to SRclientservices@nccgroup.com OR NCC Group, Attn: Client Services, 6111 Live Oak Parkway, Norcross, Georgia, 30093, USA. Telephone: 800-875-5669.

Exhibit B

Deposit Material Description

(This document must accompany each submission of Deposit Material)

Company Name		Deposit Account Number	
Deposit Name		Deposit Version	

(Deposit Name will appear in account history reports)

Deposit Media

(Please Label All Media with the Deposit Name Provided Above)

Media Type	Quantity	Media Type	Quantity
<input type="checkbox"/> CD-ROM / DVD		<input type="checkbox"/> USB Drive	
<input type="checkbox"/> DLT Tape		<input type="checkbox"/> Documentation	
<input type="checkbox"/> DAT Tape(4mm/8mm)		<input type="checkbox"/> Hard Drive / CPU	
<input type="checkbox"/> LTO Tape		<input type="checkbox"/> Circuit Board	
<input type="checkbox"/> Other (please describe):			

	Total Size of Transmission (specify in bytes)	# of Files	# of Folders
<input type="checkbox"/> Electronic Deposit			

Deposit Encryption

(Please check either "Yes" or "No" below and complete as appropriate)

Is the media or are any of the files encrypted? Yes or No

If yes, please include any passwords and decryption tools description below. Please also deposit all necessary encryption software with this deposit. Depositor at its option may submit passwords on a separate Exhibit B.

Encryption tool name		Version	
Hardware required			
Software required			
Other required information			

Deposit Certification (Please check the box below to certify and provide your contact information)

<input type="checkbox"/> I certify for Depositor that the above described Deposit Material has been transmitted electronically or sent via commercial express mail carrier to NCC Group at the address below.	<input type="checkbox"/> NCC Group has inspected and accepted the above described Deposit Material either electronically or physically. NCC Group will notify Depositor of any discrepancies.		
Print Name		Name	
Date		Date	
Email Address			
Telephone Number			

Note: If Depositor is physically sending Deposit Material to NCC Group, please label all media and mail all Deposit Material with the appropriate Exhibit B via commercial express carrier to the following address:

NCC Group
 Attn: Vault Administration
 6111 Live Oak Parkway
 Norcross, GA 30093
 Telephone: 800-875-5669

Exhibit C

Release of Deposit Material

Deposit Account Number	
------------------------	--

NCC Group will use the following procedures to process any Beneficiary Work Request to release Deposit Material. All notices under this Exhibit C shall be sent pursuant to the terms of Section 13(g) Notices.

1. Release Conditions.

Depositor and Beneficiary agree that a Work Request for the release of the Deposit Material shall be based solely on one or more of the following conditions (defined as “**Release Conditions**”):

- (i) Beneficiary’s termination of the License Agreement; or
- (ii) Failure of the Depositor to function as a going concern or operate in the ordinary course; or
- (iii) Depositor is subject to voluntary or involuntary bankruptcy.

2. Release Work Request.

A Beneficiary may submit a Work Request to NCC Group to release the Deposit Material covered under this Agreement. To the extent that the Deposit Material is subject to applicable U.S. export control regulations and laws, including ITAR, the Beneficiary Work Request to release the Deposit Material must include Beneficiary’s certification that such release would be compliant with the applicable U.S. export control regulations and laws, including ITAR. NCC Group will send a written notice of this Beneficiary Work Request within five (5) business days to the Depositor’s Authorized Person.

3. Contrary Instructions.

From the date NCC Group mails written notice of the Beneficiary Work Request to release Deposit Material covered under this Agreement, Depositor’s Authorized Person shall have ten (10) business days to deliver to NCC Group contrary instructions. Contrary instructions shall mean the written representation by Depositor that a Release Condition has not occurred or has been cured (“**Contrary Instructions**”). Contrary Instructions shall be on company letterhead and signed by a Depositor Authorized Person. Upon receipt of Contrary Instructions, NCC Group shall promptly send a copy to Beneficiary’s Authorized Person. Additionally, NCC Group shall notify both Depositor and Beneficiary Authorized Persons that there is a dispute to be resolved pursuant to the Disputes provisions of this Agreement. NCC Group will continue to store Deposit Material without release pending (i) instructions from Depositor to release the Deposit Material to Beneficiary; or (ii) dispute resolution pursuant to the Disputes provisions of this Agreement; or (iii) withdrawal of Contrary Instructions from Depositor’s Authorized Person or legal representative; or (iv) receipt of an order from a court of competent jurisdiction. The existence of a Release Condition dispute shall not relieve the Paying Party from payment of applicable Service Fees.

4. Release of Deposit Material.

If NCC Group does not receive timely Contrary Instructions from a Depositor Authorized Person or receives written instructions directly from Depositor’s Authorized Person to release a copy of the Deposit Material to the Beneficiary, NCC Group is authorized to release Deposit Material to the Beneficiary. NCC Group is entitled to receive any undisputed, unpaid Service Fees due NCC Group from the Parties before fulfilling the Work Request to release Deposit Material covered under this Agreement. Any Party may cure a default of payment of Service Fees.

5. Termination of Agreement Upon Release.

This Agreement will terminate upon the release of Deposit Material held by NCC Group.

6. Right to Use Following Release.

Beneficiary has the right under this Agreement to use the Deposit Material for the sole purpose of continuing the benefits afforded to Beneficiary by the License Agreement. Notwithstanding, the Beneficiary shall not have access to the Deposit Material unless there is a release of the Deposit Material in accordance with this Agreement. Beneficiary shall be obligated to maintain the confidentiality of the released Deposit Material.



**STATE OF MICHIGAN
ENTERPRISE PROCUREMENT**

Department of Technology, Management, and Budget
320 S. Walnut Street 2nd Floor Lansing, MI 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **3**
to
Contract Number **MA230000001706**

CONTRACTOR	Information Services Corporation
	10 Research Drive Suite 300
	Riley Meloche
	306-531-5318
	riley.meloche@isc.ca
	VS0296576

STATE	Program Manager	Various	Various
STATE	Contract Administrator	Jarrod Barron	
		517-249-0406	
		BarronJ1@michigan.gov	

CONTRACT SUMMARY

Uniform Commercial Code (UCC) System			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
November 1, 2023	November 1, 2028	5 - 12 Months	November 1, 2028
PAYMENT TERMS		DELIVERY TIMEFRAME	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-Card <input type="checkbox"/> Direct Voucher (PRC) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>		
CURRENT VALUE		VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE	
\$3,276,000.00		\$68,042.00	\$3,344,042.00	

DESCRIPTION

Effective 10/14/2024, the parties add \$68,042 for the services in the attached revised UCC implementation statement of work. All other terms, conditions, specifications, and pricing remain the same. Per contractor, agency, and DTMB Central Procurement approval.

Internal State Note: Remaining Ad Board funds after this CN: \$181,957.99.

**Program Managers
for
Multi-Agency and Statewide Contracts**

AGENCY	NAME	PHONE	EMAIL
DTMB	Daniel Klodt	517-930-6368	KlodtD@michigan.gov
MDOS	Keitha Cameron	517-231-0152	CameronK1@michigan.gov

STATEMENT OF WORK - IT CHANGE NOTICE

Project Title: UNIFORM COMMERCIAL CODE (UCC) SYSTEM	Period of Coverage: November 1 2023 thru November 1, 2028
Requesting Department: Department of State (MDOS)	Date: 10/10/2024
Agency Project Manager: Rayne Sherman	Phone: 517-275-2862
DTMB Project Manager: Mike Holka	Phone: 810-623-0557

PROJECT OBJECTIVE:

Modify payment schedule and add \$68,042.00 for implementation to accommodate extended time line of “Go-Live” of solution as a result of the Revised Project Plan.

SCOPE OF WORK:

Scope of project has not changed

REVISED PROJECT PLAN:

Key Milestones or Deliverables	Revised Scheduled Finish
Infrastructure – PROD Environment	10/8/2024
Requirements Gathering	8/6/2024
VENDOR Development	9/18/2024
VENDOR Internal Testing	10/11/2024
XML	11/15/2024
Business Partner – XML Development	9/13/2024
Business Partner Development & Configuration	9/13/2024
Business Partner – XML Testing	11/15/2024
Business Partner – XML Correction & Retesting	1/17/2025
Conversion Data Testing	10/25/2024
Run 3	10/31/2024
Business Testing – Cycle 1	10/14/2024
Final Application Configuration & Setup	10/28/2024
Final Application Configuration & Setup Testing Cycle	11/18/2024
End to End (E2E) Testing Cycle	1/23/2025
Go / No Go Decision	1/23/2025
Implementation	
Cutover	1/31/2025

PAYMENT SCHEDULE:

Revised Implementation Cost and Revised Invoice Target Dates:

Pay Point Description	Original Invoice Target Date	Revised Invoice Target Date	Pay Point Cost
Kick Off, Draft EASA Provided to SOM, 6 of 24 Requirements Gathering Sessions Completed	1/31/2024	Complete	\$70,000
Data Migration & Conversion #1 Ready for Review, DEV and TST Environments Set Up, 11 of 24 Requirements Gathering Sessions Completed	3/15/2024	Complete	\$170,000
24 of 24 Requirements Gathering Sessions Completed, Integrations in DEV and TST Environments Completed, Data Migration & Conversion #2 Ready for Review	5/13/2024	Complete	\$170,000
Completed Development of all Requirements, Functional UAT Complete	8/4/2024	11/15/2024	\$170,000
All Non-Functional Testing Complete, Data Migration and Conversion Run 3 Ready for Review, SSP Anticipate ATO by End of December	9/15/2024	12/30/2024	\$120,000
End to End Testing Complete, Training, Begin Go Live Includes XML Testing and Final Application and Set Up Testing	10/31/2024	1/23/2025	\$560,000
Hold back for 30 days post go live support	11/30/2024	2/28/2025	\$140,000
Hosting Fees for Dev and Test Environments		Upon signing Contract Change Notice	\$46,000
Additional vendor resources to support extended project implementation timeline		12/15/2024 & 1/23/2025	\$69,396 on each of these dates
Extension of initial hosting fees		11/01/2024	\$11,500
DevOps Licenses for State of MI Testing Resources		11/01/2024	\$1,230
Initial Licensing Fees		Upon signing Contract Change Notice	\$500,000
Revised Implementation Cost Total			\$2,097,522

Revised Contract Total	11/1/2023 thru 1/31/2025	2/1/2025 thru 1/31/2026	2/1/2026 thru 1/31/2027	2/1/2027 thru 1/31/2028	2/1/2028 thru 10/31/2028	11/1/2023 thru 10/31/2028
Year	Year 1.33	Year 2	Year 3	Year 4	Year .67	Total
Months	15	12	12	12	9	60
Implementation	\$1,538,792.00					\$1,538,792.00
Hosting Fees	\$57,500.00	\$55,000.00	\$55,000.00	\$61,000.00	\$50,000.00	\$278,500.00
Additional Dev Ops Licensing Fees	\$1,230.00					
Licensing Fees	\$500,000.00					\$500,000.00
Maintenance Support		\$265,000.00	\$270,000.00	\$278,000.00	\$213,750.00	\$1,026,750.00
	\$2,097,522.00	\$320,000.00	\$325,000.00	\$339,000.00	\$263,750.00	
						New contract amount
						\$3,344,042.00

PROJECT CONTACTS:

The designated Agency Project Manager is:

Rayne Sherman
 MDOS - Office of Business and Internal Services
 SOS Secondary Complex – 1st Floor
 7064 Crowner Drive
 Dimondale, MI 48821
 Phone: 517-275-2862
ShermanR@Michigan.gov

The designated DTMB Project Manager is:

Mike Holka
 DTMB – EPMO
 SOS Secondary Complex – 2nd Floor
 7064 Crowner Drive
 Dimondale, MI 48821
 Phone: 810-623-0557
HolkaM1@Michigan.gov

AGENCY RESPONSIBILITIES:

State of Michigan – Department of State responsibilities as documented and agreed to in **Contract Number 230000001706**.



STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
 Department of Technology, Management, and Budget
 320 S. WALNUT ST., LANSING, MICHIGAN 48933
 P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number 2
 to
 Contract Number 230000001706

CONTRACTOR	Information Services Corporation
	10 Research Drive , Suite 300
	Regina, SK
	Riley Meloche
	306-531-5318
	riley.meloche@isc.ca
	VS0296576

STATE	Program Manager	Various	MDOS
	Contract Administrator	Jeremy Lyon (517) 230-2858 lyonj5@michigan.gov	DTMB

CONTRACT SUMMARY

UNIFORM COMMERCIAL CODE (UCC) SYSTEM

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
November 1, 2023	November 1, 2028	5 - 1 Year	November 1, 2028

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS	EXTENDED PURCHASING
<input type="checkbox"/> P-Card <input type="checkbox"/> PRC <input type="checkbox"/> Other	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

MINIMUM DELIVERY REQUIREMENTS

--

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>		November 1, 2028

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
\$3,276,000.00	\$0.00	\$3,276,000.00

DESCRIPTION

Effective 3/8/2024, this change is to update the payment schedule and also modifying language for requirement 21. Please see the attached document for further review.

All other terms, conditions, specifications and pricing remain the same. Per contractor and agency agreement, and DTMB Central Procurement Services approval.

230000001706 - Information Service Corporation

Change Notice 2

This change is for change Notice 2, update to the payment schedule and language modified to requirement 21. Please see the payment schedule and language modification below.

	Milestone Date	Payment	
1	1/31/2024	70,000	Kick off, Draft EASA provided to SOM, 6 of 24 requirements gathering sessions completed.
2	3/15/2024	170,000	Data Migration & Conversion #1 ready for review, Dev & Test environments set up, 11 of 24 requirements gathering sessions completed.
3	5/13/2024	170,000	24 of 24 requirements gathering sessions completed, integrations in Dev/Test environments completed, Data Migration & Conversion #2 ready for review.
4	8/4/2024	170,000	Completed development of all requirements, functional UAT complete.
5	9/15/2024	120,000	All non-functional testing complete, Data Migration & Conversion Run # 3 ready for review, SSP complete.
6	10/31/2024	560,000	End-to-End testing complete, Training, Begin Go-Live.
7	11/30/2024	140,000	Hold back for 30 day Post Go-Live Support.
	Total	1,400,000	

Change to Requirement 21 on the Business Specification Worksheet

21. If not hosted by the state, the data must be stored in the government cloud (Microsoft Azure, Office 365 GCC is acceptable).



STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
 Department of Technology, Management, and Budget
 320 S. WALNUT ST., LANSING, MICHIGAN 48933
 P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number 1
 to
 Contract Number 230000001706

CONTRACTOR	Information Services Corporation
	10 Research Drive , Suite 300
	Regina, SK
	Riley Meloche
	306-531-5318
	riley.meloche@isc.ca
	VS0296576

STATE	Program Manager	Various	MULTI
	Contract Administrator	Jeremy Lyon (517) 230-2858 lyonj5@michigan.gov	DTMB

CONTRACT SUMMARY

UNIFORM COMMERCIAL CODE (UCC) SYSTEM

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
November 1, 2023	November 1, 2028	5 - 1 Year	November 1, 2028

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS	EXTENDED PURCHASING
<input type="checkbox"/> P-Card <input type="checkbox"/> PRC <input type="checkbox"/> Other	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

MINIMUM DELIVERY REQUIREMENTS

--

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>		November 1, 2028

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
\$3,276,000.00	\$0.00	\$3,276,000.00

DESCRIPTION

Effective 12/20/2023, this change is to update the project manager to Riley Meloche as the primary contact and removing Siva Ramamoorthy.

All other terms, conditions, specifications and pricing remain the same. Per contractor and agency agreement, and DTMB Central Procurement Services approval.



STATE OF MICHIGAN PROCUREMENT
 Department Of Technology, Management & Budget
 320 S. Walnut Street, Lansing, MI 48933

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. **230000001706**
 between
 THE STATE OF MICHIGAN
 and

CONTRACTOR	Information Services Corporation
	Suite 300, 10 Research Drive
	Regina, SK S4S 7J7
	Siva Ramamoorthy
	639-560-4157
	Siva.Ramamoorthy@isc.ca
	VS0296576

STATE	Program Manager	Various	
	Contract Administrator	Jeremy Lyon 517-230-2858 LyonJ5@michigan.gov	DTMB

CONTRACT SUMMARY			
DESCRIPTION: Uniform Commercial Code (UCC) System			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
11/1/2023	11/1/2028	5 – 1-year	N/A
PAYMENT TERMS		DELIVERY TIMEFRAME	
Net 45		N/A	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-card <input type="checkbox"/> Payment Request (PRC) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS			
N/A			
MISCELLANEOUS INFORMATION			
THIS IS NOT AN ORDER. This Contract Agreement is awarded on the basis of the State's inquiry bearing the solicitation number 230000000457. Orders for Delivery will be issued directly by the Departments through the issuance of a Delivery Order.			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION			\$3,276,000.00

**PROGRAM MANAGERS
FOR
MULTI-AGENCY AND STATEWIDE CONTRACTS**

AGENCY	NAME	PHONE	EMAIL
DTMB	Dan Klodt	517-930-3506	11/Klodtd@michigan.gov
MDOS	Rayne Sherman	517-275-2862	Shermanr@michigan.gov

FOR THE CONTRACTOR:

Information Services Corporation

Company Name

Authorized Agent Signature

Authorized Agent (Print or Type)

Date

FOR THE STATE:

Signature

Name & Title

DTMB – Central Procurement Services

Agency

Date

SOFTWARE CONTRACT TERMS AND CONDITIONS

These Terms and Conditions, together with all Schedules (including the Statement(s) of Work), Exhibits and any other applicable attachments or addenda (Collectively this “Contract”) are agreed to between the State of Michigan (the “**State**”) and Information Services Corporation (“**ISC**”) (“**Contractor**”), A SASKATCHEWAN CORPORATION. This Contract is effective on November 1, 2023 (“**Effective Date**”), and unless terminated, will expire on November 1, 2028 (the “**Term**”).

This Contract may be renewed for up to 5 additional 1-year period(s). Renewal is at the sole discretion of the State and will automatically extend the Term of this Contract. The State will document its exercise of renewal options via a Change Notice.

1. Definitions. For the purposes of this Contract, the following terms have the following meanings:

“**Acceptance**” has the meaning set forth in **Section 9**.

“**Acceptance Tests**” means such tests as may be conducted in accordance with **Section 9.1** and a Statement of Work to determine whether the Software meets the requirements of this Contract and the Documentation.

“**Affiliate**” of a Person means any other Person that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such Person. For purposes of this definition, the term “control” (including the terms “controlled by” and “under common control with”) means the direct or indirect ownership of more than fifty percent (50%) of the voting securities of a Person.

“**Allegedly Infringing Materials**” has the meaning set forth in **Section 18.2(b)**.

“**Approved Third Party Components**” means all third party components, including Open-Source Components, that are included in or used in connection with the Software and are specifically identified by Contractor in the Contractor’s Bid Response or as part of the State’s Security Accreditation Process defined in Schedule E – Data Security Requirements.

“**Authorized Users**” means those State personnel and service providers that are authorized by the State to access and use the Software under this Contract.

“**Business Day**” means a day other than a Saturday, Sunday or other day on which the State is authorized or required by law to be closed for business.

“**Business Requirements Specification**” means the initial specification setting forth the State’s business requirements regarding the features and functionality of the Software, as set forth in a Statement of Work.

“**Change**” has the meaning set forth in **Section 2.2**.

“**Change Notice**” has the meaning set forth in **Section 2.2(b)**.

“**Change Proposal**” has the meaning set forth in **Section 2.2(a)**.

“**Change Request**” has the meaning set forth in **Section 2.2**.

“**Confidential Information**” has the meaning set forth in **Section 22.1**.

“**Configuration**” means State-specific changes made to the Software without Source Code or structural data model changes occurring.

“**Contract**” has the meaning set forth in the preamble.

“**Contract Administrator**” is the individual appointed by each party to (a) administer the terms of this Contract, and (b) approve any Change Notices under this Contract. Each party’s Contract Administrator will be identified in Schedule A or subsequent Change Notices.

“**Contractor**” has the meaning set forth in the preamble.

“**Contractor’s Bid Response**” means the Contractor’s proposal submitted in response to the RFP.

“**Contractor Hosted**” means the Hosted Services are provided by Contractor or one or more of its Permitted Subcontractors.

“**Contractor Personnel**” means all employees of Contractor or any subcontractors or Permitted Subcontractors involved in the performance of Services hereunder.

“**Contractor Project Manager**” means the individual appointed by Contractor and identified in Schedule A or subsequent Change Notices to serve as the primary contact with regard to services, to monitor and coordinate the day-to-day activities of this

Contract, and to perform other duties as may be further defined in this Contract, including an applicable Statement of Work.

“**Customization**” means State-specific changes to the Software's underlying Source Code or structural data model changes.

“**Deliverables**” means the Software, and all other documents and other materials that Contractor is required to or otherwise does provide to the State under this Contract and otherwise in connection with any Services, including all items specifically identified as Deliverables in a Statement of Work and all Work Product.

“**Deposit Material**” refers to material required to be deposited pursuant to **Section 28**.

“**Disaster Recovery Plan**” refers to the set(s) of documents, instructions, and procedures which enable the Contractor to respond to accidents, disasters, emergencies, or threats without any stoppage or hindrance in its key operations and to the actions the Contractor takes to meet the Recovery Point and Recovery Time Objectives.

“**Documentation**” means all user manuals, operating manuals, technical manuals and any other instructions, specifications, documents or materials, in any form or media, that describe the functionality, installation, testing, operation, use, maintenance, support, technical or other components, features or requirements of the Software.

“**DTMB**” means the Michigan Department of Technology, Management and Budget.

“**End Users**” means, without limitation, members of the general public, individuals, law firms, entities, and businesses that seek access to and/or use of the Software.

“**Effective Date**” has the meaning set forth in the preamble.

“**Fees**” means the fees set forth in the Pricing Schedule attached as **Schedule B**.

“**Financial Audit Period**” has the meaning set forth in **Section 23.1**.

“**Harmful Code**” means any software, hardware or other technologies, devices or means, the purpose or effect of which is to: (a) permit unauthorized access to, or to destroy, disrupt, disable, encrypt, modify, copy, or otherwise harm or impede in any manner, any (i) computer, software, firmware, data, hardware, system or network, or (ii) any application or function of any of the foregoing or the integrity, use or operation of

any data Processed thereby; or (b) prevent the State or any Authorized User from accessing or using the Services as intended by this Contract, and includes any virus, bug, trojan horse, worm, backdoor or other malicious computer code and any time bomb or drop dead device.

“**HIPAA**” has the meaning set forth in **Section 21.1**.

“**Hosted Services**” means the hosting, management and operation of the Operating Environment, Software, other services (including support and subcontracted services), and related resources for remote electronic access and use by the State and its Authorized Users, including any services and facilities related to disaster recovery obligations.

“**Implementation Plan**” means the schedule included in a Statement of Work setting forth the sequence of events for the performance of Services under a Statement of Work, including the Milestones and Milestone Dates.

“**Integration Testing**” has the meaning set forth in **Section 9.2(a)**.

“**Intellectual Property Rights**” means all or any of the following: (a) patents, patent disclosures, and inventions (whether patentable or not); (b) trademarks, service marks, trade dress, trade names, logos, corporate names, and domain names, together with all of the associated goodwill; (c) copyrights and copyrightable works (including computer programs), mask works and rights in data and databases; (d) trade secrets, know-how and other confidential information; and (e) all other intellectual property rights, in each case whether registered or unregistered and including all applications for, and renewals or extensions of, such rights, and all similar or equivalent rights or forms of protection provided by applicable law in any jurisdiction throughout the world.

“**Key Personnel**” means any Contractor Personnel identified as key personnel in the Contract.

“**Loss or Losses**” means all losses, including but not limited to, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees and the costs of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers.

“**Maintenance Release**” means any update, upgrade, release or other adaptation or modification of the Software, including any updated Documentation, that Contractor may

generally provide to its licensees from time to time during the Term, which may contain, among other things, error corrections, enhancements, improvements or other changes to the user interface, functionality, compatibility, capabilities, performance, efficiency or quality of the Software.

“Milestone” means an event or task described in the Implementation Plan under a Statement of Work that must be completed by the corresponding Milestone Date.

“Milestone Date” means the date by which a particular Milestone must be completed as set forth in the Implementation Plan under a Statement of Work.

“New Version” means any new version of the Software, including any updated Documentation, that the Contractor may from time to time introduce and market generally as a distinct licensed product, as may be indicated by Contractor's designation of a new version number.

“Nonconformity” or **“Nonconformities”** means any failure or failures of the Software to conform to the requirements of this Contract, including any applicable Documentation.

“Open-Source Components” means any software component that is subject to any open-source copyright license agreement, including any GNU General Public License or GNU Library or Lesser Public License, or other obligation, restriction or license agreement that substantially conforms to the Open Source Definition as prescribed by the Open Source Initiative or otherwise may require disclosure or licensing to any third party of any source code with which such software component is used or compiled.

“Operating Environment” means, collectively, the platform, environment and conditions on, in or under which the Software is intended to be installed and operate, as set forth in a Statement of Work, including such structural, functional and other features, conditions and components as hardware, operating software, system architecture, configuration, computing hardware, ancillary equipment, networking, software, firmware, databases, data, and electronic systems (including database management systems).

“PAT” means a document or product accessibility template, including any Information Technology Industry Council Voluntary Product Accessibility Template or VPAT®, that specifies how information and software products, such as websites, applications, software and associated content, conform to WCAG 2.0 Level AA.

“**Permitted Subcontractor**” means any third party hired by Contractor to perform Services for the State under this Contract or have access to State Data.

“**Person**” means an individual, corporation, partnership, joint venture, limited liability company, governmental authority, unincorporated organization, trust, association or other entity.

“**Pricing Schedule**” means the schedule attached as **Schedule B**.

“**Process**” means to perform any operation or set of operations on any data, information, material, work, expression or other content, including to (a) collect, receive, input, upload, download, record, reproduce, store, organize, combine, log, catalog, cross-reference, manage, maintain, copy, adapt, alter, translate or make other improvements or derivative works, (b) process, retrieve, output, consult, use, disseminate, transmit, submit, post, transfer, disclose or otherwise provide or make available, or (c) block, erase or destroy. “**Processing**” and “**Processed**” have correlative meanings.

“**Representatives**” means a party's employees, officers, directors, partners, shareholders, agents, attorneys, successors and permitted assigns.

“**RFP**” means the State’s request for proposal designed to solicit responses for Services under this Contract.

“**Services**” means any of the services, including but not limited to, Hosted Services, Contractor is required to or otherwise does provide under this Contract.

“**Service Level Agreement**” means the schedule attached as **Schedule D**, setting forth the Support Services Contractor will provide to the State, and the parties' additional rights and obligations with respect thereto.

“**Site**” means the physical location designated by the State in, or in accordance with, this Contract or a Statement of Work for delivery and installation of the Software.

“**Software**” means Contractor’s software as set forth in a Statement of Work, and any Maintenance Releases or New Versions provided to the State and any Customizations or Configurations made by or for the State pursuant to this Contract, and all copies of the foregoing permitted under this Contract.

“Source Code” means the human readable source code of the Software to which it relates, in the programming language in which the Software was written, together with all related flow charts and technical documentation, including a description of the procedure for generating object code, all of a level sufficient to enable a programmer reasonably fluent in such programming language to understand, build, operate, support, maintain and develop modifications, upgrades, updates, adaptations, enhancements, new versions and other derivative works and improvements of, and to develop computer programs compatible with, the Software.

“Specifications” means, for the Software, the specifications collectively set forth in the Business Requirements Specification, Technical Specification, Documentation, RFP or Contractor’s Bid Response, if any, for such Software, or elsewhere in a Statement of Work.

“State” means the State of Michigan.

“State Data” has the meaning set forth in **Section 21.1**.

“State Materials” means all materials and information, including but not limited to documents, data, know-how, ideas, methodologies, specifications, software, content and technology, in any form or media, directly or indirectly provided or made available to Contractor by or on behalf of the State in connection with this Contract.

“State Program Managers” are the individuals appointed by the State, or their designees, to (a) monitor and coordinate the day-to-day activities of this Contract; (b) co-sign off on Acceptance of the Software and other Deliverables; and (c) perform other duties as may be specified in a Statement of Work. Program Managers will be identified in Schedule A or subsequent Change Notices.

“State Systems” means the information technology infrastructure, including the computers, software, databases, electronic systems (including database management systems) and networks, of the State or any of its designees.

“Statement of Work” means any statement of work entered into by the parties and incorporated into this Contract. The initial Statement of Work is attached as **Schedule A**.

“Stop Work Order” has the meaning set forth in **Section 15**.

“Support Services” means the software maintenance and support services Contractor is required to or otherwise does provide to the State under the Service Level Agreement.

“Technical Specification” means, with respect to any Software, the document setting forth the technical specifications for such Software and included in a Statement of Work.

“Term” has the meaning set forth in the preamble.

“Testing Period” has the meaning set forth in **Section 9.1(b)**.

“Transition Period” has the meaning set forth in **Section 16.3**.

“Transition Responsibilities” has the meaning set forth in **Section 16.3**.

“Unauthorized Removal” has the meaning set forth in **Section 2.5(b)**.

“Unauthorized Removal Credit” has the meaning set forth in **Section 2.5(c)**.

“User Data” means all data, information and other content of any type and in any format, medium or form, whether audio, visual, digital, screen, GUI or other, that is input, uploaded to, placed into or collected, stored, Processed, generated or output by any device, system or network by or on behalf of the State, including any and all works, inventions, data, analyses and other information and materials resulting from any use of the Software by or on behalf of the State under this Contract, except that User Data does not include the Software or data, information or content, including any GUI, audio, visual or digital or other display or output, that is generated automatically upon executing the Software without additional user input without the inclusion of user derived Information or additional user input.

“Warranty Period” means the ninety (90) calendar-day period commencing on the date of the State's Acceptance of the Software and for which Support Services are provided free of charge.

“WCAG 2.0 Level AA” means level AA of the World Wide Web Consortium Web Content Accessibility Guidelines version 2.0.

“Work Product” means all State-specific deliverables that Contractor is required to, or otherwise does, provide to the State under this Contract including but not limited to Customizations, application programming interfaces, computer scripts, macros, user

interfaces, reports, project management documents, forms, templates, and other State-specific documents and related materials together with all ideas, concepts, processes, and methodologies developed in connection with this Contract whether or not embodied in this Contract.

2. Duties of Contractor. Contractor will provide Services and Deliverables pursuant to Statement(s) of Work entered into under this Contract. Contractor will provide all Services and Deliverables in a timely, professional manner and in accordance with the terms, conditions, and Specifications set forth in this Contract and the Statement(s) of Work.

2.1 Statement of Work Requirements. No Statement of Work will be effective unless signed by each party's Contract Administrator. The term of each Statement of Work will commence on the parties' full execution of a Statement of Work and terminate when the parties have fully performed their obligations. The terms and conditions of this Contract will apply at all times to any Statements of Work entered into by the parties and incorporated into this Contract. The State will have the right to terminate such Statement of Work as set forth in **Section 16**. Contractor acknowledges that time is of the essence with respect to Contractor's obligations under each Statement of Work and agrees that prompt and timely performance of all such obligations in accordance with this Contract and the Statements of Work (including the Implementation Plan and all Milestone Dates) is strictly required.

If this Contract requires State to provide any required resources, and State fails to provide the requisite quality or quantity of such resources or fails to provide such resources in a timely manner for a period that does not exceed 10 Business Days, Contractor's sole remedy is an extension of the applicable delivery dates corresponding to the delay. Contractor's right to delay applicable delivery dates may be exercised only if Contractor provides State with reasonable notice of State's failure and Contractor uses commercially reasonable efforts to perform notwithstanding State's failure to perform.

2.2 Change Control Process. The State may at any time request in writing (each, a "**Change Request**") changes to a Statement of Work, including changes to the Services and Implementation Plan (each, a "**Change**"). Upon the State's submission of a Change Request, the parties will evaluate and implement all Changes in accordance with this **Section 2.2**.

(a) As soon as reasonably practicable, and in any case within 20 Business Days following receipt of a Change Request, Contractor will provide the State with a

written proposal for implementing the requested Change (“**Change Proposal**”), setting forth:

- (i) a written description of the proposed Changes to any Services or Deliverables, written with sufficient detail, as determined in the State’s sole discretion, to accurately describe the change being proposed;
- (ii) an amended Implementation Plan reflecting: (A) the schedule for commencing and completing any additional or modified Services or Deliverables; and (B) the effect of such Changes, if any, on completing any other Services under a Statement of Work;
- (iii) any additional State Resources Contractor deems necessary to carry out such Changes; and
- (iv) any increase or decrease in Fees resulting from the proposed Changes, which increase or decrease will reflect only the increase or decrease in time and expenses Contractor requires to carry out the Change.

(b) Within 30 Business Days following the State’s receipt of a Change Proposal, the State will by written notice to Contractor, approve, reject, or propose modifications to such Change Proposal. If the State proposes modifications, Contractor must modify and re-deliver the Change Proposal reflecting such modifications, or notify the State of any disagreement, in which event the parties will negotiate in good faith to resolve their disagreement. Upon the State’s approval of the Change Proposal or the parties’ agreement on all proposed modifications, as the case may be, the parties will execute a written agreement to the Change Proposal (“**Change Notice**”), which Change Notice will be signed by the State’s Contract Administrator and will constitute an amendment to a Statement of Work to which it relates; and

(c) If the parties fail to enter into a Change Notice within 15 Business Days following the State’s response to a Change Proposal, the State may, in its discretion:

- (i) require Contractor to perform the Services under a Statement of Work without the Change;
- (ii) require Contractor to continue to negotiate a Change Notice;
- (iii) initiate a Dispute Resolution Procedure; or

(iv) notwithstanding any provision to the contrary in a Statement of Work, terminate this Contract under **Section 16.1**.

(d) No Change will be effective until the parties have executed a Change Notice. Except as the State may request in its Change Request or otherwise in writing, Contractor must continue to perform its obligations in accordance with a Statement of Work pending negotiation and execution of a Change Notice. Contractor will use its best efforts to limit any delays or Fee increases from any Change to those necessary to perform the Change in accordance with the applicable Change Notice. Each party is responsible for its own costs and expenses of preparing, evaluating, negotiating, and otherwise processing any Change Request, Change Proposal, and Change Notice.

(e) The performance of any functions, activities, tasks, obligations, roles and responsibilities comprising the Services as described in this Contract are considered part of the Services and, thus, will not be considered a Change. This includes the delivery of all Deliverables in accordance with their respective Specifications, and the diagnosis and correction of Non-Conformities discovered in Deliverables prior to their Acceptance by the State or, subsequent to their Acceptance by the State, as necessary for Contractor to fulfill its associated warranty requirements and its Support Services under this Contract.

(f) Contractor may, on its own initiative and at its own expense, prepare and submit its own Change Request to the State. However, the State will be under no obligation to approve or otherwise respond to a Change Request initiated by Contractor.

2.3 Contractor Personnel.

(a) Contractor is solely responsible for all Contractor Personnel and for the payment of their compensation, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits.

(b) Prior to any Contractor Personnel performing any Services, Contractor will:

(i) ensure that such Contractor Personnel have the legal right to work in the United States or Canada;

(ii) Reserved

(iii) upon request, or as otherwise specified in a Statement of Work, perform background checks on all Contractor Personnel prior to their assignment. The scope is at the discretion of the State and documentation must be provided as requested. Contractor is responsible for all costs associated with the requested background checks. The State, in its sole discretion, may also perform background checks. Pursuant to Michigan law, all agencies subject to IRS Pub. 1075 are required to ask the Michigan State Police to perform fingerprint background checks on all employees, including Contractor and subcontractor employees, who may have access to any database of information maintained by the federal government that contains confidential or personal information, including, but not limited to, federal tax information. Further, pursuant to Michigan law, any agency described above is prohibited from providing Contractors or subcontractors with the result of such background check. For more information, please see Michigan Public Act 427 of 2018.

(c) Contractor and all Contractor Personnel will comply with all rules, regulations, and policies of the State that are communicated to Contractor in writing, including security procedures concerning systems and data and remote access, building security procedures, including the restriction of access by the State to certain areas of its premises or systems, and general health and safety practices and procedures.

(d) The State reserves the right to require the removal of any Contractor Personnel found, in the judgment of the State, to be unacceptable. The State's request must be written with reasonable detail outlining the reasons for the removal request. Replacement personnel for the removed person must be fully qualified for the position. If the State exercises this right, and Contractor cannot immediately replace the removed personnel, the State agrees to negotiate an equitable adjustment in schedule or other terms that may be affected by the State's required removal.

2.4 Contractor Project Manager. Throughout the Term of this Contract, Contractor must maintain a Contractor employee acceptable to the State to serve as Contractor Project Manager, who will be considered Key Personnel of Contractor.

(a) Contractor Project Manager must:

(i) have the requisite authority, and necessary skill, experience, and qualifications, to perform in such capacity;

(ii) be responsible for overall management and supervision of Contractor's performance under this Contract; and

(iii) be the State's primary point of contact for communications with respect to this Contract, including with respect to giving and receiving all day-to-day approvals and consents.

(b) Contractor Project Manager must attend all regularly scheduled meetings as set forth in the Implementation Plan and will otherwise be available as set forth in a Statement of Work.

(c) Contractor will maintain the same Contractor Project Manager throughout the Term of this Contract, unless:

(i) the State requests in writing the removal of Contractor Project Manager;

(ii) the State consents in writing to any removal requested by Contractor in writing;

(iii) Contractor Project Manager ceases to be employed by Contractor, whether by resignation, involuntary termination or otherwise.

(d) Contractor will promptly replace its Contractor Project Manager on the occurrence of any event set forth in **Section 2.4(c)**. Such replacement will be subject to the State's prior written approval.

2.5 Contractor's Key Personnel.

(a) The State has the right to recommend and approve in writing the initial assignment, as well as any proposed reassignment or replacement, of any Key Personnel. Before assigning an individual to any Key Personnel position, Contractor will notify the State of the proposed assignment, introduce the individual to the State Program Managers or their designees, and provide the State with a resume and any other information about the individual reasonably requested by the State. The State reserves the right to interview the individual before granting written approval. In the event the State finds a proposed individual unacceptable, the State will provide a written explanation including reasonable detail outlining the reasons for the rejection.

(b) Contractor will not remove any Key Personnel from their assigned roles on this Contract without the prior written consent of the State. The Contractor's removal of Key Personnel without the prior written consent of the State is an unauthorized removal ("**Unauthorized Removal**"). An Unauthorized Removal

does not include replacing Key Personnel for reasons beyond the reasonable control of Contractor, including illness, disability, leave of absence, personal emergency circumstances, resignation, or for cause termination of the Key Personnel's employment. Any Unauthorized Removal may be considered by the State to be a material breach of this Contract, in respect of which the State may elect to terminate this Contract for cause under **Section 16.1**.

(c) It is further acknowledged that an Unauthorized Removal will interfere with the timely and proper completion of this Contract, to the loss and damage of the State, and that it would be impracticable and extremely difficult to determine and remedy the actual damage sustained by the State as a result of any Unauthorized Removal. Therefore, Contractor and the State agree that in the case of any Unauthorized Removal in respect of which the State does not elect to exercise its rights under **Section 16**, Contractor will issue to the State an amount equal to \$25,000 per individual (each, an "**Unauthorized Removal Credit**").

(d) Contractor acknowledges and agrees that each of the Unauthorized Removal Credits assessed under **Subsection 2.5(c)** above: (i) is a reasonable estimate of and compensation for the anticipated or actual harm to the State that may arise from the Unauthorized Removal, which would be impossible or very difficult to accurately estimate; and (ii) may, at the State's option, be credited or set off against any Fees or other charges payable to Contractor under this Contract.

2.6 Subcontractors. Contractor must obtain prior written approval of the State, which consent may be given or withheld in the State's sole discretion, before engaging any Permitted Subcontractor to provide Services to the State under this Contract. Third parties otherwise retained by Contractor to provide Contractor or other clients of contractor with services are not Permitted Subcontractors, and therefore do not require prior approval by the State. Engagement of any subcontractor or Permitted Subcontractor by Contractor does not relieve Contractor of its representations, warranties or obligations under this Contract. Without limiting the foregoing, Contractor will:

(a) be responsible and liable for the acts and omissions of each such subcontractor (including such Permitted Subcontractor and Permitted Subcontractor's employees who, to the extent providing Services or Deliverables, will be deemed Contractor Personnel) to the same extent as if such acts or omissions were by Contractor or its employees;

(b) name the State a third-party beneficiary under Contractor’s Contract with each Permitted Subcontractor with respect to the Services;

(c) be responsible for all fees and expenses payable to, by or on behalf of each Permitted Subcontractor in connection with this Contract, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits; and

(d) notify the State of the location of the Permitted Subcontractor and indicate if it is located within the continental United States.

3. Notices. All notices and other communications required or permitted under this Contract must be in writing and will be considered given and received: (a) when verified by written receipt if sent by courier; (b) when actually received if sent by mail without verification of receipt; or (c) when verified by automated receipt or electronic logs if sent by facsimile or email.

If to State:	If to Contractor:
Jeremy Lyon 320 S. Walnut Street Lansing, MI 48909 LyonJ5@michigan.gov 517-230-2858	Information Services Corporation 300 – 10 Research Drive Regina, Saskatchewan S4S 7J7 legalnotices@isc.ca (306) 787-8179

4. Insurance. Contractor must maintain the minimum insurances identified in the Insurance Schedule attached as **Schedule C**.

5. Software License.

5.1 Perpetual License. Contractor hereby grants to the State and its Authorized Users a non-exclusive, royalty-free, perpetual, irrevocable right and license to use the Software and Documentation in accordance with the terms and conditions of this Contract solely for the purpose set out in Schedule A or Statements of Work, which includes, at no additional cost, the right to use the Software without any limitation as to the number of Authorized Users and End Users, provided that:

(a) The State is prohibited from reverse engineering, disassembling, or decompiling the Software or any part thereof, making derivative works, modifying, adapting or copying the Software (the foregoing prohibition includes but is not limited to review of data structures or similar materials produced by programs), or access or use the Software in order to build or support, and/or assist a third party in building or supporting, products or services competitive to

the Contractor except as is expressly permitted by this Contract or required to be permitted by law;

(b) The State is authorized to make copies of the Software for backup, disaster recovery, and archival purposes;

(c) The State is authorized to make copies of the Software to establish a test environment to conduct Acceptance Testing;

(d) Title to and ownership of the Software shall at all times remain with Contractor and/or its licensors, as applicable; and

(e) Except as expressly agreed in writing or as provided in the Contract, the State is not permitted to sub-license the use of the Software or any accompanying Documentation or to sell, rent, lease, transfer, assign, distribute, display, host, outsource, disclose, permit timesharing or service bureau use, or otherwise commercially exploit or make the Software or Documentation available to any third party not specified in the Contract.

(f) End Users will have the right to use and access the Software for as long as the license to the Software is in effect.

5.2 Additional License Restrictions.

a. The State agrees that it may not, unless expressly permitted within the Contract:

- i. knowingly use or permit use of the Software including by uploading, emailing, posting, publishing or otherwise transmitting any material, for any purpose intended to constitute an infringement of intellectual property or other proprietary rights, or otherwise violate any applicable laws, ordinances or regulations; or
- ii. knowingly remove or modify any Contractor markings or any notice of Contractor's proprietary rights without the Contractor's consent.

b. The State further agrees that neither it nor its Authorized Users shall:

- i. knowingly send or store viruses, worms, time bombs, trojan horses or other harmful or malicious: code, files, scripts, agents or programs; or
- ii. knowingly interfere with or cause a material disruption to the integrity or performance of the Software.

5.3 Certification. To the extent that a License granted to the State is not unlimited, Contractor may request written certification from the State regarding use of the Software for the sole purpose of verifying compliance with this **Section 5**. Such written certification may occur no more than once in any 24 month period during the Term of the Contract. The State will respond to any such request within 45 calendar days of receipt. If the State's use is greater than contracted, Contractor may invoice the State for any unlicensed use (and related support) pursuant to the terms of this Contract at the rates set forth in **Schedule B**, and the unpaid license and support fees shall be payable in accordance with the terms of the Contract. Payment under this provision shall be Contractor's sole and exclusive remedy to cure these issues.

5.4 State License Grant to Contractor. The State hereby grants to Contractor a limited, non-exclusive, non-transferable license (i) to use the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos, solely in accordance with the State's specifications, and (ii) to display, reproduce, distribute and transmit in digital form the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos in connection with promotion of the Services as communicated to Contractor by the State. Use of the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos will be specified in the applicable Statement of Work. Contractor is provided a limited license to State Materials for the sole and exclusive purpose of providing the Services.

6. Third Party Components. At least 30 days prior to adding new Third Party Components, Contractor will provide the State with notification information identifying and describing the addition. Throughout the Term, on an annual basis, Contractor will provide updated information identifying and describing any Approved Third Party Components included in the Software.

7. Intellectual Property Rights

7.1 Ownership Rights in Software

- (a) For purposes of this **Section 7** only, the term "Software" does not include Customizations.

(b) Subject to the rights and licenses granted by Contractor in this Contract and the provisions of **Section 7.1(c)**:

(i) Contractor and/or its licensors, as applicable, reserves and retains its entire right, title and interest in and to all Intellectual Property Rights arising out of or relating to the Software; and

(ii) none of the State or Authorized Users or End Users acquire any ownership of Intellectual Property Rights in or to the Software or Documentation as a result of this Contract.

(c) As between the State, on the one hand, and Contractor, on the other hand, the State has, reserves and retains, sole and exclusive ownership of all right, title and interest in and to State Materials, User Data, including all Intellectual Property Rights arising therefrom or relating thereto.

7.2 The State is and will be the sole and exclusive owner of all right, title, and interest in and to all Work Product developed exclusively for the State under this Contract, including all Intellectual Property Rights. In furtherance of the foregoing:

(a) Contractor will create all Work Product as work made for hire as defined in Section 101 of the Copyright Act of 1976; and

(b) to the extent any Work Product, or Intellectual Property Rights do not qualify as, or otherwise fails to be, work made for hire, Contractor hereby:

(i) assigns, transfers, and otherwise conveys to the State, irrevocably and in perpetuity, throughout the universe, all right, title, and interest in and to such Work Product, including all Intellectual Property Rights; and

(ii) irrevocably waives any and all claims Contractor may now or hereafter have in any jurisdiction to so-called “moral rights” or rights of *droit moral* with respect to the Work Product.

8. Software Implementation.

8.1 Implementation. Contractor will as applicable; deliver, install, configure, integrate, and otherwise provide and make fully operational the Software on or prior to the applicable Milestone Date in accordance with the criteria set forth in a Statement of Work and the Implementation Plan.

8.2 Site Preparation. Unless otherwise set forth in a Statement of Work, Contractor is responsible for ensuring the relevant Operating Environment is set up and in working order to allow Contractor to deliver and install the Software on or prior to

the applicable Milestone Date. Contractor will provide the State with such notice as is specified in a Statement of Work, prior to delivery of the Software to give the State sufficient time to prepare for Contractor's delivery and installation of the Software. If the State is responsible for Site preparation, Contractor will provide such assistance as the State requests to complete such preparation on a timely basis.

9. Software Acceptance Testing.

9.1 Acceptance Testing.

(a) Unless otherwise specified in a Statement of Work, upon installation of the Software, or in the case of Contractor Hosted Software, when Contractor notifies the State in writing that the Hosted Services are ready for use in a production environment, Acceptance Tests will be conducted as set forth in this **Section 9** to ensure the Software conforms to the requirements of this Contract, including the applicable Specifications and Documentation.

(b) All Acceptance Tests will take place at the designated Site(s) in the Operating Environment described in a Statement of Work, commence within 10 Business Days following installation of the Software, or the receipt by the State of the notification in **Section 9.1(a)**, and be conducted diligently for up to 30 Business Days, or such other period as may be set forth in a Statement of Work (the "**Testing Period**"). Acceptance Tests will be conducted by the State, and Contractor will make suitable Contractor Personnel available to observe or participate in such Acceptance Tests; and

9.2 Contractor is solely responsible for all costs and expenses related to Contractor's participation in and observation of Acceptance Testing.

(a) Upon delivery and installation of any application programming interfaces, Configuration or Customizations, or any other applicable Work Product, to the Software under a Statement of Work, additional Acceptance Tests will be performed on the modified Software as a whole to ensure full operability, integration, and compatibility among all elements of the Software ("**Integration Testing**"). Integration Testing is subject to all procedural and other terms and conditions set forth in this **Section 9**.

(b) The State may suspend Acceptance Tests and the corresponding Testing Period by written notice to Contractor if the State discovers a material Non-Conformity in the tested Software or part or feature of the Software. In such event, Contractor will immediately, and in any case within 10 Business Days,

correct such Non-Conformity, whereupon the Acceptance Tests and Testing Period will resume for the balance of the Testing Period.

9.3 Notices of Completion, Non-Conformities, and Acceptance. Within 15 Business Days following the completion of any Acceptance Tests, including any Integration Testing, the State will prepare and provide to the other party written notice of the completion of the tests. Such notice describing in reasonable detail the tests conducted and the results of such tests, including any uncorrected Non-Conformity in the tested Software.

(a) If such notice is provided by either party and identifies any Non-Conformities, the parties' rights, remedies, and obligations will be as set forth in **Section 9.4** and **Section 9.5**.

(b) If such notice is provided by the State, is signed by the State Program Managers or their designees, and identifies no Non-Conformities, such notice constitutes the State's Acceptance of such Software.

9.4 Failure of Acceptance Tests. If Acceptance Tests identify any Non-Conformities, Contractor, at Contractor's sole cost and expense, will remedy all such Non-Conformities and re-deliver the Software, in accordance with the requirements set forth in the Contract. Redelivery will occur as promptly as commercially possible and, in any case, within 30 Business Days following, as applicable, Contractor's receipt of the State's notice under **Section 9.1(a)** identifying any Non-Conformities.

9.5 Repeated Failure of Acceptance Tests. If Acceptance Tests identify any Non-Conformity in the Software after a third or subsequent delivery of the Software, or Contractor fails to re-deliver the Software on a timely basis, the State may, in its sole discretion, by written notice to Contractor:

(a) continue the process set forth in this **Section 9**;

(b) accept the Software as a nonconforming deliverable, in which case the Fees for such Software will be reduced equitably to reflect the value of the Software as received relative to the value of the Software had it conformed; or

(c) deem the failure to be a non-curable material breach of this Contract and a Statement of Work and terminate this Contract for cause in accordance with **Section 16.1**.

9.6 Acceptance. Acceptance ("**Acceptance**") of the Software (subject, where applicable, to the State's right to Integration Testing) will occur on the date that is

the earliest of the State's delivery of a notice accepting the Software under **Section 9.3(b)**.

10. Non-Software Acceptance.

10.1 All other non-Software Services and Deliverables are subject to inspection and testing by the State within 30 calendar days of the State's receipt of them ("State Review Period"), unless otherwise provided in the Statement of Work. If the non-Software Services and Deliverables are not fully accepted by the State, the State will notify Contractor by the end of the State Review Period that either: (a) the non-Software Services and Deliverables are accepted but noted deficiencies must be corrected; or (b) the non-Software Services and Deliverables are rejected. If the State finds material deficiencies, it may: (i) reject the non-Software Services and Deliverables without performing any further inspections; (ii) demand performance at no additional cost; or (iii) terminate this Contract in accordance with **Section 16.1**, Termination for Cause, if Contractor fails to cure the material deficiencies within the time period provided by the State for any such material deficiencies the State deems are curable.

10.2 Within 10 business days from the date of Contractor's receipt of notification of acceptance with deficiencies or rejection of any non-Software Services and Deliverables, Contractor must cure, at no additional cost, the deficiency and deliver unequivocally acceptable non-Software Services and Deliverables to the State. If acceptance with deficiencies or rejection of the non-Software Services and Deliverables impacts the content or delivery of other non-completed non-Software Services and Deliverables, the parties' respective Program Managers must determine an agreed to number of days for re-submission that minimizes the overall impact to the Contract. However, nothing herein affects, alters, or relieves Contractor of its obligations to correct deficiencies in accordance with the time response standards set forth in this Contract.

10.3 If Contractor is unable or refuses to correct a material deficiency within the time response standards set forth in this Contract, the State may cancel the order in whole or in part. The State, or a third party identified by the State, may provide the non-Software Services and Deliverables and recover the difference between the cost to cure and the Contract price plus an additional 10% administrative fee.

11. Assignment. Contractor may not assign this Contract to any other party without the prior approval of the State. Upon notice to Contractor, the State, in its sole discretion, may assign in whole or in part, its rights or responsibilities under this Contract to any other party. If the State determines that a novation of the Contract to a third party is necessary,

Contractor will agree to the novation and provide all necessary documentation and signatures.

12. Change of Control. Contractor will notify the State, within 30 days of any public announcement or otherwise once legally permitted to do so, of a change in Contractor's organizational structure or ownership. For purposes of this Contract, a change in control means any of the following:

- (a) a sale of more than 50% of Contractor's stock;
- b) a sale of substantially all of Contractor's assets;
- (c) a change in a majority of Contractor's board members;
- (d) consummation of a merger or consolidation of Contractor with any other entity;
- (e) a change in ownership through a transaction or series of transactions;
- (f) or the board (or the stockholders) approves a plan of complete liquidation.

A change of control does not include any consolidation or merger effected exclusively to change the domicile of Contractor, or any transaction or series of transactions principally for bona fide equity financing purposes. In the event of a change of control, Contractor must require the successor to assume this Contract and all of its obligations under this Contract.

13. Invoices and Payment.

13.1 Invoices must conform to the requirements communicated from time-to-time by the State. All undisputed amounts are payable within 45 days of the State's receipt. Contractor may only charge for Services and Deliverables provided as specified in Statement(s) of Work. Invoices must include an itemized statement of all charges.

13.2 The State has the right to withhold payment of any disputed amounts until the parties agree as to the validity of the disputed amount. The State will notify Contractor of any dispute within a reasonable time. Payment by the State will not constitute a waiver of any rights as to Contractor's continuing obligations, including claims for deficiencies or substandard Services and Deliverables. Contractor's acceptance of final payment by the State constitutes a waiver of all claims by

Contractor against the State for payment under this Contract, other than those claims previously filed in writing on a timely basis and still disputed.

13.3 The State will only disburse payments under this Contract through Electronic Funds Transfer (EFT). Contractor must register with the State at <http://www.michigan.gov/SIGMAVSS> to receive electronic fund transfer payments. If Contractor does not register, the State is not liable for failure to provide payment.

13.4 Right of Setoff. Without prejudice to any other right or remedy it may have, the State reserves the right to set off at any time any amount then due and owing to it by Contractor against any amount payable by the State to Contractor under this Contract.

13.5 Taxes. The State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if Services or Deliverables purchased under this Contract are for the State's exclusive use. Notwithstanding the foregoing, all Fees are exclusive of taxes, and Contractor is responsible for all sales, use and excise taxes, and any other similar taxes, duties and charges of any kind imposed by any federal, state, or local governmental entity on any amounts payable by the State under this Contract.

13.6 Pricing/Fee Changes. All Pricing set forth in this Contract will not be increased, except as otherwise expressly provided in this Section.

(a) The Fees will not be increased at any time except for the addition of additional licenses, the fees for which licenses will also remain firm in accordance with the Pricing set forth in the Pricing Schedule.

(b) Reserved

14. Liquidated Damages.

14.1 The parties understand and agree that any liquidated damages (which includes but is not limited to applicable credits) set forth in this Contract are reasonable estimates of the State's damages in accordance with applicable law.

14.2 The parties acknowledge and agree that Contractor could incur liquidated damages for more than one event.

14.3 The assessment of liquidated damages will not constitute a waiver or release of any other remedy the State may have under this Contract for Contractor's breach of this Contract, including without limitation, the State's right to terminate this Contract for cause under **Section 16.1** and the State will be entitled in its discretion

to recover actual damages caused by Contractor's failure to perform its obligations under this Contract. However, the State will reduce such actual damages by the amounts of liquidated damages received for the same events causing the actual damages.

14.4 Amounts due the State as liquidated damages may be set off against any Fees payable to Contractor under this Contract, or the State may bill Contractor as a separate item and Contractor will promptly make payments on such bills.

15. Stop Work Order. The State may suspend any or all activities under the Contract at any time. The State will provide Contractor a written stop work order detailing the suspension. Contractor must comply with the stop work order upon receipt. Within 90 calendar days, or any longer period agreed to by Contractor, the State will either:

- (a) issue a notice authorizing Contractor to resume work, or
- (b) terminate the Contract or delivery order. The State will not pay for activities that have been suspended, Contractor's lost profits, or any additional compensation during a stop work period.

16. Termination, Expiration, Transition. The State may terminate this Contract, the Support Services, or any Statement of Work, in accordance with the following:

16.1 Termination for Cause. In addition to any right of termination set forth elsewhere in this Contract:

- (a) The State may terminate this Contract for cause, in whole or in part, if Contractor, as determined by the State:
 - i) endangers the value, integrity, or security of State Systems, State Data, or the State's facilities or personnel;
 - (ii) becomes insolvent, petitions for bankruptcy court proceedings, or has an involuntary bankruptcy proceeding filed against it by any creditor; or
 - (iii) breaches any of its material duties or obligations under this Contract. Any reference to specific breaches being material breaches within this Contract will not be construed to mean that other breaches are not material.
- (b) If the State terminates this Contract under this **Section 16.1**, the State will issue a termination notice specifying whether Contractor must:

(i) cease performance immediately. Contractor must submit all invoices for Services accepted by the State within 30 days of the date of termination. Failure to submit an invoice within that timeframe will constitute a waiver by Contractor for any amounts due to Contractor for Services accepted by the State under this Contract, or

(ii) continue to perform for a specified period. If it is later determined that Contractor was not in breach of this Contract, the termination will be deemed to have been a termination for convenience, effective as of the same date, and the rights and obligations of the parties will be limited to those provided in **Section 16.2**.

(c) The State will only pay for amounts due to Contractor for Services accepted by the State on or before the date of termination, subject to the State's right to set off any amounts owed by the Contractor for the State's reasonable costs in terminating this Contract. Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination, including any prepaid Fees. Contractor must pay all reasonable costs incurred by the State in terminating this Contract for cause, including administrative costs, attorneys' fees, court costs, transition costs, and any costs the State incurs to procure the Services from other sources.

16.2 Termination for Convenience. The State may:

(a) immediately terminate this Contract in whole or in part, without penalty, due to appropriation or budget shortfalls; or

(b) terminate this Contract for any reason other than appropriation or budget shortfalls on providing thirty (30) calendar days' written notice to the Contractor.

The termination notice will specify whether Contractor must:

(i) cease performance immediately. Contractor must submit all invoices for Services accepted by the State within 30 days of the date of termination. Failure to submit an invoice within that timeframe will constitute a waiver by Contractor for any amounts due to Contractor for Services accepted by the State under this Contract, or

(ii) continue to perform in accordance with **Section 16.3**. If the State terminates this Contract for convenience, the State will pay all reasonable costs, as determined by the State, for State approved Transition Responsibilities to the extent the funds are available.

16.3 Transition Responsibilities.

(a) Upon termination or expiration of this Contract for any reason, Contractor must, for a period of time specified by the State (not to exceed 180 calendar days; the “**Transition Period**”), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the Contract to continue without interruption or adverse effect, and to facilitate the orderly transfer of the Services to the State or its designees. Such transition assistance may include but is not limited to:

- (i) continuing to perform the Services at the established Contract rates;
- (ii) taking all reasonable and necessary measures to transition performance of the work, including all applicable Services to the State or the State’s designee;
- (iii) taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, and comply with **Section 22.5** regarding the return or destruction of State Data at the conclusion of the Transition Period; and
- (iv) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts (collectively, the “**Transition Responsibilities**”). The Term of this Contract is automatically extended through the end of the Transition Period.

(b) Contractor will follow the transition plan attached as **Schedule G** as it pertains to both transition in and transition out activities.

17. Indemnification

17.1 General Indemnification. Contractor must defend, indemnify and hold the State, its departments, divisions, agencies, offices, commissions, officers, and employees harmless, without limitation, from and against any and all actions, claims, losses, liabilities, damages, costs, attorney fees, and expenses (including those required to establish the right to indemnification), arising out of or relating to:

- (a) any breach by Contractor (or any of Contractor’s employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable) of any of the promises, agreements, representations, warranties, or insurance requirements contained in this Contract;

(b) any infringement, misappropriation, or other violation of any Intellectual Property Right or other right of any third party;

(c) any bodily injury, death, or damage to real or tangible personal property occurring wholly or in part due to action or inaction by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable); and

(d) any acts or omissions of Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable).

17.2 Indemnification Procedure. The State will notify Contractor in writing if indemnification is sought; however, failure to do so will not relieve Contractor, except to the extent that Contractor is materially prejudiced. Contractor must, to the satisfaction of the State, demonstrate its financial ability to carry out these obligations. The State is entitled to:

(a) regular updates on proceeding status;

(b) participate in the defense of the proceeding;

(c) employ its own counsel; and to

(d) retain control of the defense, at its own cost and expense, if the State deems necessary. Contractor will not, without the State's prior written consent (not to be unreasonably withheld), settle, compromise, or consent to the entry of any judgment in or otherwise seek to terminate any claim, action, or proceeding. Any litigation activity on behalf of the State or any of its subdivisions, under this **Section 17** Error! Reference source not found., must be coordinated with the Department of Attorney General. An attorney designated to represent the State may not do so until approved by the Michigan Attorney General and appointed as a Special Assistant Attorney General.

17.3 The State is constitutionally prohibited from indemnifying Contractor or any third parties.

18. Infringement Remedies.

18.1 The remedies set forth in this Section are in addition to, and not in lieu of, all other remedies that may be available to the State under this Contract or otherwise, including the State's right to be indemnified for such actions.

18.2 If any Software or any component thereof, other than State Materials, is found to be infringing or if any use of any Software or any component thereof is enjoined, threatened to be enjoined or otherwise the subject of an infringement claim, Contractor must, at Contractor's sole cost and expense:

- (a) procure for the State the right to continue to use such Software or component thereof to the full extent contemplated by this Contract; or
- (b) modify or replace the materials that infringe or are alleged to infringe ("**Allegedly Infringing Materials**") to make the Software and all of its components non-infringing while providing fully equivalent features and functionality.

18.3 If neither of the foregoing is possible notwithstanding Contractor's best efforts, then Contractor may direct the State to cease any use of any materials that have been enjoined or finally adjudicated as infringing, provided that Contractor will:

- (a) refund to the State all amounts paid by the State in respect of such Allegedly Infringing Materials and any other aspects of the Software provided under a Statement of Work for the Allegedly Infringing Materials that the State cannot reasonably use as intended under this Contract; and
- (b) in any case, at its sole cost and expense, secure the right for the State to continue using the Allegedly Infringing Materials for a transition period of up to 6 months to allow the State to replace the affected features of the Software without disruption.

18.4 If Contractor directs the State to cease using any Software under **Section 18.3**, the State may terminate this Contract for cause under **Section 16.1**. Unless the claim arose against the Software independently of any of the actions specified below, Contractor will have no liability for any claim of infringement arising solely from:

- (a) Contractor's compliance with any designs, specifications, or instructions of the State; or
- (b) modification of the Software by the State without the prior knowledge and approval of Contractor.

19. Disclaimer of Damages and Limitation of Liability.

19.1 The State's Disclaimer of Damages. THE STATE WILL NOT BE LIABLE, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT,

NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT FOR CONSEQUENTIAL, INCIDENTAL, INDIRECT, OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST PROFITS AND LOST BUSINESS OPPORTUNITIES.

19.2 The State's Limitation of Liability. IN NO EVENT WILL THE STATE'S AGGREGATE LIABILITY TO CONTRACTOR UNDER THIS CONTRACT, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT, EXCEED THE MAXIMUM AMOUNT OF FEES PAYABLE UNDER THIS CONTRACT.

19.3 The Contractor's Limitation of Liability. EXCEPT AS PROVIDED IN SUBSECTION 19.4, IN NO EVENT WILL THE CONTRACTOR'S AGGREGATE LIABILITY TO THE STATE UNDER THIS CONTRACT, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT, EXCEED THE AMOUNT OF 200% OF THE FEES PAYABLE BY THE STATE TO THE CONTRACTOR UNDER THIS CONTRACT.

19.4 The limitation of liability set forth in subsection 19.3 does not apply to (i) Contractor's obligation to indemnify under this Contract; (ii) Contractor's obligations under this Contract pertaining to Loss or Compromise of State Data, (iii) any loss or claim to the extent the loss or claim is covered by a policy of insurance maintained, or required by this Contract to be maintained, by Contractor; and (iv) damages arising from Contractor's gross negligence or intentional misconduct.

20. Disclosure of Litigation, or Other Proceeding. Contractor must notify the State within 14 calendar days of receiving notice of any litigation, investigation, arbitration, or other proceeding (collectively, "**Proceeding**") involving Contractor, a Permitted Subcontractor, or an officer or director of Contractor or Permitted Subcontractor, that arises during the term of the Contract, including:

- (a) a criminal Proceeding;
- (b) a parole or probation Proceeding;
- (c) a Proceeding under the Sarbanes-Oxley Act;
- (d) a civil Proceeding involving:

- (i) a claim that might reasonably be expected to adversely affect Contractor's viability or financial stability; or
- (ii) a governmental or public entity's claim or written allegation of fraud; or
- (e) a Proceeding involving any license that Contractor is required to possess in order to perform under this Contract.

21. State Data.

21.1 Ownership. The State's data ("**State Data**"), which will be treated by Contractor as Confidential Information, includes:

- (a) User Data; and
- (b) any other data collected, used, Processed, stored, or generated in connection with the Services, including but not limited to:
 - (i) personally identifiable information ("**PII**") collected, used, Processed, stored, or generated as the result of the Services, including, without limitation, any information that identifies an individual, such as an individual's social security number or other government-issued identification number, date of birth, address, telephone number, biometric data, mother's maiden name, email address, credit card information, or an individual's name in combination with any other of the elements here listed; and
 - (ii) protected health information ("**PHI**") collected, used, Processed, stored, or generated as the result of the Services, which is defined under the Health Insurance Portability and Accountability Act ("**HIPAA**") and its related rules and regulations.

21.2 State Data is and will remain the sole and exclusive property of the State and all right, title, and interest in the same is reserved by the State.

21.3 Contractor Use of State Data. Contractor is provided a limited license to State Data for the sole and exclusive purpose of providing the Services, including a license to collect, process, store, generate, and display State Data only to the extent necessary in the provision of the Services. Contractor must:

- (a) keep and maintain State Data in strict confidence, using such degree of care as is appropriate and consistent with its obligations as further described in this Contract and applicable law to avoid unauthorized access, use, disclosure, or loss;

(b) use and disclose State Data solely and exclusively for the purpose of providing the Services, such use and disclosure being in accordance with this Contract, any applicable Statement of Work, and applicable law;

(c) keep and maintain State Data in the continental United States and

(d) not use, sell, rent, transfer, mine, distribute, commercially exploit, or otherwise disclose or make available State Data for Contractor's own purposes or for the benefit of anyone other than the State without the State's prior written consent. Contractor's misuse of State Data may violate state or federal laws, including but not limited to MCL 752.795.

21.4 Discovery. Contractor will immediately notify the State upon receipt of any requests which in any way might reasonably require access to State Data or the State's use of the Software and Hosted Services, if applicable. Contractor will notify the State Program Managers or their designees by the fastest means available and also in writing. In no event will Contractor provide such notification more than twenty-four (24) hours after Contractor receives the request. Contractor will not respond to subpoenas, service of process, FOIA requests, and other legal requests related to the State without first notifying the State and obtaining the State's prior approval of Contractor's proposed responses. Contractor agrees to provide its completed responses to the State with adequate time for State review, revision and approval.

21.5 Loss or Compromise of Data. In the event of any act, error or omission, negligence, misconduct, or breach on the part of Contractor that compromises or is suspected to compromise the security, confidentiality, integrity, or availability of State Data or the physical, technical, administrative, or organizational safeguards put in place by Contractor that relate to the protection of the security, confidentiality, or integrity of State Data, Contractor must, as applicable:

(a) notify the State as soon as practicable but no later than 24 hours of becoming aware of such occurrence;

(b) cooperate with the State in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by the State;

(c) in the case of PII or PHI, at the State's sole election:

(i) with approval and assistance from the State, notify the affected individuals who comprise the PII or PHI as soon as practicable but no later

than is required to comply with applicable law, or, in the absence of any legally required notification period, within 5 calendar days of the occurrence; or

(ii) reimburse the State for any costs in notifying the affected individuals;

(d) in the case of PII, provide third-party credit and identity monitoring services to each of the affected individuals who comprise the PII for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than 24 months following the date of notification to such individuals;

(e) perform or take any other actions required to comply with applicable law as a result of the occurrence;

(f) pay for any costs associated with the occurrence, including but not limited to any costs incurred by the State in investigating and resolving the occurrence, including reasonable attorney's fees associated with such investigation and resolution;

(g) without limiting Contractor's obligations of indemnification as further described in this Contract, indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the occurrence;

(h) be responsible for recreating lost State Data in the manner and on the schedule set by the State without charge to the State; and

(i) provide to the State a detailed plan within 10 calendar days of the occurrence describing the measures Contractor will undertake to prevent a future occurrence. Notification to affected individuals, as described above, must comply with applicable law, be written in plain language, not be tangentially used for any solicitation purposes, and contain, at a minimum: name and contact information of Contractor's representative; a description of the nature of the loss; a list of the types of data involved; the known or approximate date of the loss; how such loss may affect the affected individual; what steps Contractor has taken to protect the affected individual; what steps the affected individual can take to protect himself or herself; contact information for major credit card reporting agencies; and, information regarding the credit and identity monitoring services to be provided by Contractor. Notification to affected individuals must be reviewed and approved by the State in writing prior to its delivery.

Notification to any other party, including but not limited to public media outlets, must also be reviewed and approved by the State in writing prior to its dissemination.

21.6 The parties agree that any damages relating to a breach of this **Section 21** are to be considered direct damages and not consequential damages.

22. Non-Disclosure of Confidential Information. The parties acknowledge that each party may be exposed to or acquire communication or data of the other party that is confidential, privileged communication not intended to be disclosed to third parties.

22.1 Meaning of Confidential Information. For the purposes of this Contract, the term “**Confidential Information**” means all information and documentation of a party that: (a) has been marked “confidential” or with words of similar meaning, at the time of disclosure by such party; (b) if disclosed orally or not marked “confidential” or with words of similar meaning, was subsequently summarized in writing by the disclosing party and marked “confidential” or with words of similar meaning; and, (c) should reasonably be recognized as confidential information of the disclosing party. The term “Confidential Information” does not include any information or documentation that was: (a) subject to disclosure under the Michigan Freedom of Information Act (FOIA); (b) already in the possession of the receiving party without an obligation of confidentiality; (c) developed independently by the receiving party, as demonstrated by the receiving party, without violating the disclosing party’s proprietary rights; (d) obtained from a source other than the disclosing party without an obligation of confidentiality; or, (e) publicly available when received, or thereafter became publicly available (other than through any unauthorized disclosure). For purposes of this Contract, in all cases and for all matters, State Data is deemed to be Confidential Information.

22.2 Obligation of Confidentiality. The parties agree to hold all Confidential Information in strict confidence and not to copy, reproduce, sell, transfer, or otherwise dispose of, give or disclose such Confidential Information to third parties other than employees, agents, or subcontractors of a party who have a need to know in connection with this Contract or to use such Confidential Information for any purposes whatsoever other than the performance of this Contract. The parties agree to advise and require their respective employees, agents, and subcontractors of their obligations to keep all Confidential Information confidential. Disclosure to the Contractor’s subcontractor is permissible where:

(a) the subcontractor is a Permitted Subcontractor;

(b) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the Permitted Subcontractor's responsibilities; and

(c) Contractor obligates the Permitted Subcontractor in a written contract, where possible, to maintain the State's Confidential Information in confidence. At the State's request, any of the Contractor's and Permitted Subcontractor's Representatives may be required to execute a separate agreement to be bound by the provisions of this **Section 22.2**.

22.3 Cooperation to Prevent Disclosure of Confidential Information. Each party must use its best efforts to assist the other party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the foregoing, each party must advise the other party immediately in the event either party learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Contract. Each party will cooperate with the other party in seeking injunctive or other equitable relief against any such person.

22.4 Remedies for Breach of Obligation of Confidentiality. Each party acknowledges that breach of its obligation of confidentiality may give rise to irreparable injury to the other party, which damage may be inadequately compensable in the form of monetary damages. Accordingly, a party may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies which may be available, to include, in the case of the State, at the sole election of the State, the immediate termination, without liability to the State, of this Contract or any Statement of Work corresponding to the breach or threatened breach.

22.5 Surrender of Confidential Information upon Termination. Upon termination or expiration of this Contract or a Statement of Work, in whole or in part, each party must, within 15 Business Days from the date of termination, return to the other party any and all Confidential Information received from the other party, or created or received by a party on behalf of the other party, which are in such party's possession, custody, or control. Upon confirmation from the State, of receipt of all data, Contractor must permanently sanitize or destroy the State's Confidential Information, including State Data, from all media including backups using National Security Agency ("NSA") and/or National Institute of Standards and Technology ("NIST") (NIST Guide for Media Sanitization 800-88) data sanitization methods or as otherwise instructed by the State. If the State determines that the return of any Confidential Information is not feasible or necessary, Contractor must destroy the

Confidential Information as specified above. The Contractor must certify the destruction of Confidential Information (including State Data) in writing within 5 Business Days from the date of confirmation from the State.

23. Records Maintenance, Inspection, Examination, and Audit.

23.1 Right of Audit. Pursuant to MCL 18.1470, the State or its designee may audit Contractor to verify compliance with this Contract. Contractor must retain and provide to the State or its designee and the auditor general upon request, all financial and accounting records related to this Contract through the Term of this Contract and for 4 years after the latter of termination, expiration, or final payment under this Contract or any extension (“**Financial Audit Period**”). If an audit, litigation, or other action involving the records is initiated before the end of the Financial Audit Period, Contractor must retain the records until all issues are resolved.

23.2 Right of Inspection. Within 10 calendar days of providing notice, the State and its authorized representatives or designees have the right to enter and inspect Contractor’s premises or any other places where Services are being performed, and examine, copy, and audit all records related to this Contract. Contractor must cooperate and provide reasonable assistance. If financial errors are revealed, the amount in error must be reflected as a credit or debit on subsequent invoices until the amount is paid or refunded. Any remaining balance at the end of this Contract must be paid or refunded within 45 calendar days.

23.3 Application. This **Section 23** applies to Contractor, any Affiliate, and any Permitted Subcontractor that performs Services in connection with this Contract.

24. Support Services. Contractor will provide the State with the Support Services described in the Service Level Agreement attached as **Schedule D** to this Contract. Such Support Services will be provided:

- (a) Free of charge during the Warranty Period.
- (b) Thereafter, for so long as the State elects to receive Support Services for the Software, in consideration of the State's payment of Fees for such services in accordance with the rates set forth in the Pricing Schedule.

25. Data Security Requirements. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will maintain and enforce an information security program including safety and physical and technical security policies and procedures with respect to its Processing of the State’s

Confidential Information that comply with the requirements of the State's data security policies as set forth in **Schedule E** to this Contract.

26. Training. Contractor will provide, at no additional charge, training on all uses of the Software permitted hereunder in accordance with the times, locations and other terms set forth in a Statement of Work. Upon the State's request, Contractor will timely provide training for additional Authorized Users or other additional training on all uses of the Software for which the State requests such training, at such reasonable times and locations and pursuant to such rates and other terms as are set forth in the Pricing Schedule.

27. Maintenance Releases; New Versions

27.1 Maintenance Releases. Provided that the State is current on its Fees, during the Term, Contractor will provide the State, at no additional charge, with all Maintenance Releases, each of which will constitute Software and be subject to the terms and conditions of this Contract.

27.2 New Versions. Provided that the State is current on its Fees, during the Term, Contractor will provide the State, at no additional charge, with all New Versions, each of which will constitute Software and be subject to the terms and conditions of this Contract.

27.3 Installation. The State has no obligation to install or use any Maintenance Release or New Versions. If the State wishes to install any Maintenance Release or New Version, the State will have the right to have such Maintenance Release or New Version installed, in the State's discretion, by Contractor or other authorized party as set forth in a Statement of Work. Contractor will provide the State, at no additional charge, adequate Documentation for installation of the Maintenance Release or New Version, which has been developed and tested by Contractor and Acceptance Tested by the State. The State's decision not to install or implement a Maintenance Release or New Version of the Software will not affect its right to receive Support Services throughout the Term of this Contract.

28. Source Code Escrow

28.1 Escrow Contract. The parties may enter into a separate intellectual property escrow agreement. Such escrow agreement will govern all aspects of Source Code escrow and release. The cost of the escrow will be the sole responsibility of Contractor.

28.2 Deposit. Within 30 business days of the Go-Live, Contractor will deposit with the escrow agent, pursuant to the procedures of the escrow agreement, the Source Code for the Software, as well as the Documentation and names and contact information for each author or other creator of the Software. At least semi-annually, or after a major release of any update, upgrade, or enhancement to the Software, unless otherwise agreed by the parties, Contractor will deposit updated Source Code, documentation, names, and contact information with the escrow agent.

28.3 Verification. At State's request and expense, the escrow agent may at any time verify the Deposit Material, including without limitation by compiling Source Code, comparing it to the Software, and reviewing the completeness and accuracy of any and all material. In the event that the Deposit Material does not conform to the requirements of **Section 28** above:

- (a) Contractor will promptly deposit conforming Deposit Material; and
- (b) Contractor will pay the escrow agent for subsequent verification of the new Deposit Material. Any breach of the provisions of this **Section 28.3** will constitute material breach of this Contract, and no further payments will be due from the State until such breach is cured, in addition to other remedies the State may have.

28.4 Deposit Material License. Contractor hereby grants the State a license to use, reproduce, and create derivative works from the Deposit Material, provided the State may not distribute or sublicense the Deposit Material or make any use of it whatsoever except for such internal or governmental uses as necessary to maintain and support the Software. Copies of the Deposit Material created or transferred pursuant to this Contract are licensed, not sold, and the State receives no title to or ownership of any copy or of the Deposit Material itself. The Deposit Material constitutes Confidential Information of Contractor pursuant to **Section 22** (Non-disclosure of Confidential Information) of this Contract (provided no provision of **Section 22.4** calling for return of Confidential Information before termination of this Contract will apply to the Deposit Material).

28.5 Provision of Source Code. Notwithstanding any escrow agreement, within 10 Business Days of the State's written request or the termination of this Contract for any reason, the Contractor will provide to the State, in a format and manner specified by the State, a copy of the most recent version of the Deposit Material.

29. Contractor Representations and Warranties.

29.1 Authority. Contractor represents and warrants to the State that:

- (a) It is duly organized, validly existing, and in good standing as a corporation or other entity as represented under this Contract under the laws and regulations of its jurisdiction of incorporation, organization, or chartering;
- (b) It has the full right, power, and authority to enter into this Contract, to grant the rights and licenses granted under this Contract, and to perform its contractual obligations;
- (c) The execution of this Contract by its Representative has been duly authorized by all necessary organizational action; and
- (d) When executed and delivered by Contractor, this Contract will constitute the legal, valid, and binding obligation of Contractor, enforceable against Contractor in accordance with its terms.
- (e) Contractor is neither currently engaged in nor will engage in the boycott of a person based in or doing business with a strategic partner as described in 22 USC 8601 to 8606.

29.2 Bid Response. Contractor represents and warrants to the State that:

- (a) The prices proposed by Contractor were arrived at independently, without consultation, communication, or agreement with any other Bidder for the purpose of restricting competition; the prices quoted were not knowingly disclosed by Contractor to any other Bidder to the RFP; and no attempt was made by Contractor to induce any other Person to submit or not submit a proposal for the purpose of restricting competition;
- (b) All written information furnished to the State by or for Contractor in connection with this Contract, including Contractor's Bid Response, is true, accurate, and complete, and contains no untrue statement of material fact or omits any material fact necessary to make the information not misleading;
- (c) Contractor is not in material default or breach of any other contract or agreement that it may have with the State or any of its departments, commissions, boards, or agencies. Contractor further represents and warrants that it has not been a party to any contract with the State or any of its departments that was terminated by the State within the previous 5 years for the reason that Contractor failed to perform or otherwise breached an obligation of the contract; and

(d) If any of the certifications, representations, or disclosures made in Contractor's Bid Response change after contract award, the Contractor is required to report those changes immediately to the Contract Administrator.

29.3 Software Representations and Warranties. Contractor further represents and warrants to the State that:

(a) it is the legal and beneficial owner of the entire right, title and interest in and to the Software, including all Intellectual Property Rights relating thereto;

(b) it has, and throughout the license term, will retain the unconditional and irrevocable right, power and authority to grant and perform the license hereunder;

(c) it has, and throughout the Term and any additional periods during which Contractor does or is required to perform the Services will have, the unconditional and irrevocable right, power and authority, including all permits and licenses required, to provide the Services and grant and perform all rights and licenses granted or required to be granted by it under this Contract;

(e) neither its grant of the license, nor its performance under this Contract does or to its knowledge will at any time:

(i) conflict with or violate any applicable law;

(ii) require the consent, approval or authorization of any governmental or regulatory authority or other third party; or

(iii) require the provision of any payment or other consideration to any third party;

(f) when used by the State or any Authorized User in accordance with this Contract and the Documentation, the Software, the Hosted Services, if applicable, or Documentation as delivered or installed by Contractor does not or will not:

(i) infringe, misappropriate, or otherwise violate any Intellectual Property Right or other right of any third party; or

(ii) fail to comply with any applicable law;

(g) as provided by Contractor, the Software and Services do not and will not at any time during the Term contain any:

- (i) Harmful Code; or
 - (ii) Third party or Open-Source Components that operate in such a way that it is developed or compiled with or linked to any third party or Open-Source Components, other than Approved Third Party Components specifically described in a Statement of Work.
- (h) all Documentation is and will be complete and accurate in all material respects when provided to the State such that at no time during the license term will the Software have any material undocumented feature; and
- (i) it will perform all Services in a timely, skillful, professional and workmanlike manner in accordance with commercially reasonable industry standards and practices for similar services, using personnel with the requisite skill, experience and qualifications, and will devote adequate resources to meet its obligations under this Contract.
- (j) when used in the Operating Environment (or any successor thereto) in accordance with the Documentation, all Software as provided by Contractor, will be fully operable, meet all applicable specifications, and function in all respects, in conformity with this Contract and the Documentation;
- (k) Contractor acknowledges that the State cannot indemnify any third parties, including but not limited to any third-party software providers that provide software that will be incorporated in or otherwise used in conjunction with the Services, and that notwithstanding anything to the contrary contained in any third-party software license agreement or end user license agreement, the State will not indemnify any third party software provider for any reason whatsoever;
- (l) no Maintenance Release or New Version, when properly installed in accordance with this Contract, will have a material adverse effect on the functionality or operability of the Software.
- (m) all Configurations or Customizations made during the Term will be forward-compatible with future Maintenance Releases or New Versions and be fully supported without additional costs.
- (n) If Contractor Hosted:
 - (i) Contractor will not advertise through the Hosted Services (whether with adware, banners, buttons or other forms of online advertising) or link to external web sites that are not approved in writing by the State;

(ii) the Software and Services will in all material respects conform to and perform in accordance with the Specifications and all requirements of this Contract, including the Availability and Availability Requirement provisions set forth in the Service Level Agreement;

(iii) all Specifications are, and will be continually updated and maintained so that they continue to be current, complete and accurate and so that they do and will continue to fully describe the Hosted Services in all material respects such that at no time during the Term or any additional periods during which Contractor does or is required to perform the Services will the Hosted Services have any material undocumented feature;

(o) During the Term of this Contract, any audit rights contained in any third-party software license agreement or end user license agreement for third-party software incorporated in or otherwise used in conjunction with the Software or with the Hosted Services, if applicable, will apply solely to Contractor or its Permitted Subcontractors. Regardless of anything to the contrary contained in any third-party software license agreement or end user license agreement, third-party software providers will have no audit rights whatsoever against State Systems or networks.

29.4 Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THIS CONTRACT, CONTRACTOR HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH RESPECT TO THIS CONTRACT.

30. Offers of Employment. During the first 12 months of the Contract, should Contractor hire an employee of the State, without prior written consent of the State, who has substantially worked on any project covered by this Contract, the Contractor will be billed for 50% of the employee's annual salary in effect at the time of separation.

31. Conflicts and Ethics. Contractor will uphold high ethical standards and is prohibited from: (a) holding or acquiring an interest that would conflict with this Contract; (b) doing anything that creates an appearance of impropriety with respect to the award or performance of the Contract; (c) attempting to influence or appearing to influence any State employee by the direct or indirect offer of anything of value; or (d) paying or agreeing to pay any person, other than employees and consultants working for Contractor, any consideration contingent upon the award of the Contract. Contractor must immediately notify the State of any violation or potential violation of these standards. This Section applies to Contractor, any parent, affiliate, or subsidiary

organization of Contractor, and any Permitted Subcontractor that provides Services and Deliverables in connection with this Contract.

32. Compliance with Laws. Contractor, its subcontractors, including Permitted Subcontractors, and their respective Representatives must comply with all laws in connection with this Contract.

33. Nondiscrimination. Under the Elliott-Larsen Civil Rights Act, 1976 PA 453, MCL 37.2101, *et seq.*, the Persons with Disabilities Civil Rights Act, 1976 PA 220, MCL 37.1101, *et seq.*, and Executive Directive [2019-09](#), Contractor and its subcontractors agree not to discriminate against an employee or applicant for employment with respect to hire, tenure, terms, conditions, or privileges of employment, or a matter directly or indirectly related to employment, because of race, color, religion, national origin, age, sex, height, weight, marital status, partisan considerations, any mental or physical disability, or genetic information that is unrelated to the person's ability to perform the duties of a particular job or position. Breach of this covenant is a material breach of the Contract.

34. Unfair Labor Practice. Under MCL 423.324, the State may void any Contract with a Contractor or Permitted Subcontractor who appears on the Unfair Labor Practice register compiled under MCL 423.322.

35. Governing Law. This Contract is governed, construed, and enforced in accordance with Michigan law, excluding choice-of-law principles, and all claims relating to or arising out of this Contract are governed by Michigan law, excluding choice-of-law principles. Any dispute arising from this Contract must be resolved in the Michigan Court of Claims. Complaints against the State must be initiated in Ingham County, Michigan. Contractor waives any objections, such as lack of personal jurisdiction or *forum non conveniens*. Contractor must appoint an agent in Michigan to receive service of process.

36. Non-Exclusivity. Nothing contained in this Contract is intended nor is to be construed as creating any requirements contract with Contractor, nor does it provide Contractor with a right of first refusal for any future work. This Contract does not restrict the State or its agencies from acquiring similar, equal, or like Services from other sources.

37. Force Majeure

37.1 Force Majeure Events. Neither party will be liable or responsible to the other party, or be deemed to have defaulted under or breached the Contract, for any failure or delay in fulfilling or performing any term hereof, when and to the extent

such failure or delay is caused by: acts of God, flood, fire or explosion, war, terrorism, invasion, riot or other civil unrest, embargoes or blockades in effect on or after the date of the Contract, national or regional emergency, or any passage of law or governmental order, rule, regulation or direction, or any action taken by a governmental or public authority, including imposing an embargo, export or import restriction, quota or other restriction or prohibition (each of the foregoing, a “**Force Majeure Event**”), in each case provided that: (a) such event is outside the reasonable control of the affected party; (b) the affected party gives prompt written notice to the other party, stating the period of time the occurrence is expected to continue; (c) the affected party uses diligent efforts to end the failure or delay and minimize the effects of such Force Majeure Event.

37.2 State Performance; Termination. In the event of a Force Majeure Event affecting Contractor’s performance under the Contract, the State may suspend its performance hereunder until such time as Contractor resumes performance. The State may terminate the Contract by written notice to Contractor if a Force Majeure Event affecting Contractor’s performance hereunder continues substantially uninterrupted for a period of 10 Business Days or more. Unless the State terminates the Contract pursuant to the preceding sentence, any date specifically designated for Contractor’s performance under the Contract will automatically be extended for a period up to the duration of the Force Majeure Event.

37.3 Exclusions; Non-suspended Obligations. Notwithstanding the foregoing or any other provisions of the Contract or this Schedule:

(a) in no event will any of the following be considered a Force Majeure Event:

(i) shutdowns, disruptions or malfunctions of Hosted Services or any of Contractor’s telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to the Hosted Services; or

(ii) the delay or failure of any Contractor Personnel to perform any obligation of Contractor hereunder unless such delay or failure to perform is itself by reason of a Force Majeure Event.

(b) no Force Majeure Event modifies or excuses Contractor’s obligations under **Section 21** (State Data), **22** (Non-Disclosure of Confidential Information), or **17** (Indemnification) of the Contract, Disaster Recovery and Backup requirements set forth in the Service Level Agreement, Availability Requirement (if Contractor

Hosted) defined in the Service Level Agreement, or any data retention or security requirements under the Contract.

38. Dispute Resolution. The parties will endeavor to resolve any Contract dispute in accordance with this provision. The dispute will be referred to the parties' respective Contract Administrators or Program Managers. Such referral must include a description of the issues and all supporting documentation. The parties must submit the dispute to a senior executive if unable to resolve the dispute within 15 business days. The parties will continue performing while a dispute is being resolved, unless the dispute precludes performance. A dispute involving payment does not preclude performance. Litigation to resolve the dispute will not be instituted until after the dispute has been elevated to the parties' senior executive and either concludes that resolution is unlikely or fails to respond within 15 business days. The parties are not prohibited from instituting formal proceedings: (a) to avoid the expiration of statute of limitations period; (b) to preserve a superior position with respect to creditors; or (c) where a party makes a determination that a temporary restraining order or other injunctive relief is the only adequate remedy. This Section does not limit the State's right to terminate the Contract.

39. Media Releases. News releases (including promotional literature and commercial advertisements, or any endorsement on contractor's websites) pertaining to this Contract or project to which it relates must not be made without the prior written approval of the State, and then only in accordance with the explicit written instructions of the State.

40. Severability. If any part of this Contract is held invalid or unenforceable, by any court of competent jurisdiction, that part will be deemed deleted from this Contract and the severed part will be replaced by agreed upon language that achieves the same or similar objectives. The remaining Contract will continue in full force and effect.

41. Waiver. Failure to enforce any provision of this Contract will not constitute a waiver.

42. Survival. Any right, obligation, or condition that, by its express terms or nature and context is intended to survive, will survive the termination or expiration of this Contract; such rights, obligations, or conditions include, but are not limited to, those related to transition responsibilities; indemnification; disclaimer of damages and limitations of liability; State Data; non-disclosure of Confidential Information; representations and warranties; insurance and bankruptcy.

43. Administrative Fee and Reporting Contractor must pay an administrative fee of 1% on all payments made to Contractor under the Contract including transactions with MiDEAL members, and other states (including governmental subdivisions and

authorized entities). Administrative fee payments must be made online by check or credit card at: <https://www.thepayplace.com/mi/dtmb/adminfee>

Contractor must submit an itemized purchasing activity report, which includes at a minimum, the name of the purchasing entity and the total dollar volume in sales. Reports should be mailed to MiDeal@michigan.gov.

The administrative fee and purchasing activity report are due within 30 calendar days from the last day of each calendar quarter.

44. Extended Purchasing Program. This contract is extended to MiDEAL members. MiDEAL members include local units of government, school districts, universities, community colleges, and nonprofit hospitals. A current list of MiDEAL members is available at www.michigan.gov/mideal.

Upon written agreement between the State and Contractor, this contract may also be extended to: (a) other states (including governmental subdivisions and authorized entities) and (b) State of Michigan employees.

If extended, Contractor must supply all Contract Activities at the established Contract prices and terms. The State reserves the right to impose an administrative fee and negotiate additional discounts based on any increased volume generated by such extensions.

Contractor must submit invoices to, and receive payment from, extended purchasing program members on a direct and individual basis.

45. Contract Modification. This Contract may not be amended except by signed agreement between the parties (a “**Contract Change Notice**”). Notwithstanding the foregoing, no subsequent Statement of Work or Contract Change Notice executed after the Effective Date will be construed to amend this Contract unless it specifically states its intent to do so and cites the section or sections amended.

46. HIPAA Compliance. The State and Contractor must comply with all obligations under HIPAA and its accompanying regulations, including but not limited to entering into a business associate agreement, if reasonably necessary to keep the State and Contractor in compliance with HIPAA.

47. Accessibility Requirements.

47.1 All Software provided by Contractor under this Contract, including associated content and documentation, must conform to WCAG 2.0 Level AA. Contractor must

provide a description of conformance with WCAG 2.0 Level AA specifications by providing a completed PAT for each product provided under the Contract. At a minimum, Contractor must comply with the WCAG 2.0 Level AA conformance claims it made to the State, including the level of conformance provided in any PAT. Throughout the Term of the Contract, Contractor must:

- (a) maintain compliance with WCAG 2.0 Level AA and meet or exceed the level of conformance provided in its written materials, including the level of conformance provided in each PAT;
- (b) comply with plans and timelines approved by the State to achieve conformance in the event of any deficiencies;
- (c) ensure that no Maintenance Release, New Version, update or patch, when properly installed in accordance with this Contract, will have any adverse effect on the conformance of Contractor's Software to WCAG 2.0 Level AA;
- (d) promptly respond to and resolve any complaint the State receives regarding accessibility of Contractor's Software;
- (e) upon the State's written request, provide evidence of compliance with this Section by delivering to the State Contractor's most current PAT for each product provided under the Contract; and
- (f) participate in the State of Michigan Digital Standards Review described below.

47.2 State of Michigan Digital Standards Review. Contractor must assist the State, at no additional cost, with development, completion, and on-going maintenance of an accessibility plan, which requires Contractor, upon request from the State, to submit evidence to the State to validate Contractor's accessibility and compliance with WCAG 2.0 Level AA. Prior to the solution going-live and thereafter on an annual basis, or as otherwise required by the State, re-assessment of accessibility may be required. At no additional cost, Contractor must remediate all issues identified from any assessment of accessibility pursuant to plans and timelines that are approved in writing by the State.

47.3 Warranty. Contractor warrants that all WCAG 2.0 Level AA conformance claims made by Contractor pursuant to this Contract, including all information provided in any PAT Contractor provides to the State, are true and correct. If the State determines such conformance claims provided by the Contractor represent a

higher level of conformance than what is actually provided to the State, Contractor will, at its sole cost and expense, promptly remediate its Software to align with Contractor's stated WCAG 2.0 Level AA conformance claims in accordance with plans and timelines that are approved in writing by the State. If Contractor is unable to resolve such issues in a manner acceptable to the State, in addition to all other remedies available to the State, the State may terminate this Contract for cause under **Section 16.1**.

47.4 Contractor must, without limiting Contractor's obligations of indemnification as further described in this Contract, indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State arising out of its failure to comply with the foregoing accessibility standards

47.5 Failure to comply with the requirements in this **Section 47** shall constitute a material breach of this Contract.

48. Further Assurances. Each party will, upon the reasonable request of the other party, execute such documents and perform such acts as may be necessary to give full effect to the terms of this Contract.

49. Relationship of the Parties. The relationship between the parties is that of independent contractors. Contractor, its employees, and agents will not be considered employees of the State. No partnership or joint venture relationship is created by virtue of this Contract. Contractor, and not the State, is responsible for the payment of wages, benefits and taxes of Contractor's employees and any subcontractors. Prior performance does not modify Contractor's status as an independent contractor. Neither party has authority to contract for nor bind the other party in any manner whatsoever.

50. Headings. The headings in this Contract are for reference only and do not affect the interpretation of this Contract.

51. No Third-party Beneficiaries. This Contract is for the sole benefit of the parties and their respective successors and permitted assigns. Nothing herein, express or implied, is intended to or will confer on any other person or entity any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this Contract.

52. Equitable Relief. Each party to this Contract acknowledges and agrees that (a) a breach or threatened breach by such party of any of its obligations under this Contract may give rise to irreparable harm to the other party for which monetary damages would not be an adequate remedy and (b) in the event of a breach or a threatened breach by

such party of any such obligations, the other party hereto is, in addition to any and all other rights and remedies that may be available to such party at law, at equity or otherwise in respect of such breach, entitled to equitable relief, including a temporary restraining order, an injunction, specific performance and any other relief that may be available from a court of competent jurisdiction, without any requirement to post a bond or other security, and without any requirement to prove actual damages or that monetary damages will not afford an adequate remedy. Each party to this Contract agrees that such party will not oppose or otherwise challenge the appropriateness of equitable relief or the entry by a court of competent jurisdiction of an order granting equitable relief, in either case, consistent with the terms of this Section.

53. Effect of Contractor Bankruptcy. Subject to Canadian law, all rights and licenses granted by Contractor under this Contract are and will be deemed to be rights and licenses to “intellectual property,” and all Software and Deliverables are and will be deemed to be “embodiments” of “intellectual property,” for purposes of, and as such terms are used in and interpreted under, Section 365(n) of the United States Bankruptcy Code (the “**Code**”). If Contractor or its estate becomes subject to any bankruptcy or similar proceeding, the State retains and has the right to fully exercise all rights, licenses, elections, and protections under this Contract, the Code and all other applicable bankruptcy, insolvency, and similar laws with respect to all Software and other Deliverables. Without limiting the generality of the foregoing and subject to Canadian law, Contractor acknowledges and agrees that, if Contractor or its estate will become subject to any bankruptcy or similar proceeding:

(a) all rights and licenses granted to the State under this Contract will continue subject to the terms and conditions of this Contract, and will not be affected, even by Contractor’s rejection of this Contract; and

(b) the State will be entitled to a complete duplicate of (or complete access to, as appropriate) all such intellectual property and embodiments of intellectual property comprising or relating to any Software or other Deliverables, and the same, if not already in the State’s possession, will be promptly delivered to the State, unless Contractor elects to and does in fact continue to perform all of its obligations under this Contract.

54. Schedules. All Schedules that are referenced herein and attached hereto are hereby incorporated by reference. The following Schedules are attached hereto and incorporated herein:

Schedule A	Statement of Work
Schedule B	Pricing Schedule

Schedule C	Insurance Schedule
Schedule D	Service Level Agreement
Schedule E	Data Security Requirements
Schedule F	Disaster Recovery Plan (if Contractor Hosted)
Schedule G	Transition Plan

55. Counterparts. This Contract may be executed in counterparts, each of which will be deemed an original, but all of which together are deemed to be one and the same agreement and will become effective and binding upon the parties as of the Effective Date at such time as all the signatories hereto have signed a counterpart of this Contract. A signed copy of this Contract delivered by facsimile, e-mail or other means of electronic transmission (to which a signed copy is attached) is deemed to have the same legal effect as delivery of an original signed copy of this Contract.

56. Entire Agreement. These Terms and Conditions, including all Statements of Work and other Schedules and Exhibits (again collectively the “Contract”) constitutes the sole and entire agreement of the parties to this Contract with respect to the subject matter contained herein, and supersedes all prior and contemporaneous understandings and agreements, representations and warranties, both written and oral, with respect to such subject matter. In the event of any inconsistency between the statements made in the Terms and Conditions, the Schedules, Exhibits, and a Statement of Work, the following order of precedence governs: (a) first, these Terms and Conditions and (b) second, Schedule E – Data Security Requirements and (c) third, each Statement of Work; and (d) fourth, the remaining Exhibits and Schedules to this Contract. **NO TERMS ON CONTRACTOR’S INVOICES, WEBSITE, BROWSE-WRAP, SHRINK-WRAP, CLICK-WRAP, CLICK-THROUGH OR OTHER NON-NEGOTIATED TERMS AND CONDITIONS PROVIDED WITH ANY OF THE SERVICES, OR DOCUMENTATION HEREUNDER, EVEN IF ATTACHED TO STATE’S DELIVERY OR PURCHASE ORDER, WILL CONSTITUTE A PART OR AMENDMENT OF THIS CONTRACT OR IS BINDING ON THE STATE OR ANY AUTHORIZED USER FOR ANY PURPOSE. ALL SUCH OTHER TERMS AND CONDITIONS HAVE NO FORCE AND EFFECT AND ARE DEEMED REJECTED BY THE STATE AND THE AUTHORIZED USER, EVEN IF ACCESS TO OR USE OF SUCH SERVICE OR DOCUMENTATION REQUIRES AFFIRMATIVE ACCEPTANCE OF SUCH TERMS AND CONDITIONS.**

SCHEDULE A – STATEMENT OF WORK

1. DEFINITIONS

The following terms have the meanings set forth below. All initial capitalized terms that are not defined in this Schedule will have the respective meanings given to them in Section 1 of the Contract Terms and Conditions.

Term	Definition
CEPAS	Centralized Electronic Payment Authorization System The State of Michigan approved electronic solution for the receipt of credit/debit card and electronic check through the automated clearing house.
EASA	Enterprise Architecture Solution Assessment All Contractor proposals and new contracts must be accompanied by an Assessment, documenting the architectural details of the proposed solution.
IACA	International Association of Commercial Administrators
MILogin	MILogin is the State of Michigan’s centralized identity management solution that allows users the ability to access many state services and systems online across multiple state agencies, using a single user ID and password.
PSP	Policies, Standards, and Procedures; DTMB’s IT policies and product standards are foundationally based on federal and state laws, contracts, and industry “best practices” for the development, use, and protection of state assets and intellectual property. Technology policies and product standards are published using a) departmental policy and standard documents, b) Service Catalogs produced by various IT divisions/bureaus, and c) industry Best Practices adopted by internal IT groups.
Public User	Non-State of Michigan employee users. These users may be individuals, an institution or an employee of an institution such as a bank.
SOM	State of Michigan

SSP	<p>System Security Plan</p> <p>Overview of the information system and security requirements including information assets, security categorization, applicable laws and regulations, system interconnections, information sharing, system dependencies, network diagrams, network devices and components, system hardware, system software, data flow diagrams, implementation of the security controls. Describes the controls in place or planned to be in place required to provide the appropriate level of security.</p>
State of Michigan User	Also referred to as internal, this includes MDOS and DTMB employees that use/support the UCC system.
SUITE	<p>State Unified Information Technology Environment</p> <p>The State’s project management and system engineering methodologies are key components of the SUITE framework. SUITE is based on industry best practices and provides in-depth guidance for the entire project life cycle.</p>
UCC	Uniform Commercial Code
Work Order	Term unique to current system, it is a unique order number assigned to each batch of purchase, utilized for tracking purposes.

2. BACKGROUND

Since 1964, the Michigan Department of State (MDOS) has been responsible for filing and maintaining financing statements on secured transactions under Article 9 of the UCC, as adopted in Michigan.

The UCC unit handles the duties and functions of Article 9 and provides a central location in Michigan for filing public notice of secured transactions. The public notice, called a financing statement, is evidence of a commercial agreement between two or more parties. The UCC Unit also makes all financing statement records available to the public for searching by debtor name or document number. When a business applicant pledges collateral on a loan, UCC search results tell lenders whether others have filed a claim against the same collateral. The UCC Unit’s operations and system are governed, by statute, Michigan Uniform Commercial Code Public Act 1974 of 1962.

3. PURPOSE

The State is contracting for a solution that will increase online filing to 100% and enhance what is available for UCC. The solution must be available 24 hours a day, 7 days a week for filing and searching of finance statements, federal tax liens, state tax liens and unemployment liens.

The new UCC solution must:

- Enable customers greater flexibility submitting filings online
- Have additional functionality to include ability to accept attachments through online and XML portals
- Allow staff review of online filings prior to acceptance
- Redaction functionality to enable staff to redact SSN and FEIN included with filing materials
- The system must allow customers to pay online via redirection to CEPAS payment system or billing account via API connections to CARS
- XML must allow eCheck payments with secure CEPAS ID
- Provide ability for staff, management, and financial staff to run reports

The Solution will not require social security numbers. PII laws have been included to protect any inappropriately submitted SSNs or PII.

Contractor solutions must follow the following State and Federal laws:

Federal Laws

- Fair Credit Reporting Act
- Privacy Act of 1974 – 5 U.S.C. § 552a

State of Michigan Laws:

- Uniform Commercial Code Act 174 of 1962
- UCC Administrative Rules
- MCL 257.307 (11) (Disclosure/Display of SSN)
- MCL 257.40b “Personal information” and “highly restricted personal information” defined
- MCL 257.208c Disclosure of personal information
- MCL 257.903 False certification as felony
- Identity Theft Protection Act, Act 452 of 2004, as amended
- Social Security Number Privacy Act, Public Act 454 of 2004, as amended
- MCL 28.291a, Personal Identification Cards (Personal Information, highly restricted personal information definitions)
- MCL 28.295a, Personal Identification Cards (Penalty for Misuse)
- MCL 28.298, Personal Identification Cards (Personal Information Disclosure)

The State is contracting for a Commercial Off the Shelf (COTS), Contractor Hosted Software Solution and applicable Services.

The information stored in this system is Public but could include Confidential data. Potential confidential business information (FEIN), financial information, personal information, personally identifiable information are submitted to the UCC system. Specific elements may include:

- Social Security Number – not required but submitted by user error
- State Tax Information (Personal or Business)
- Email and Telephone numbers, including home, business, mobile and other personal numbers associated with a user account
- Payment confirmation # as required by PCI compliance
- Federal tax liens
- Unemployment liens
- First name, Last Name, Middle Name
- Address
- Personal Assets such as information identifying personally owned property
- Network Asset Information, such as Internet Protocol (IP)

4. IT ENVIRONMENT RESPOSIBILITIES

Contractor will meet components and will maintain compliance with the requirements of **Schedule E – Data Security Requirements**

For a Contractor Hosted Software Solution:

Definitions:

Facilities – Physical buildings containing Infrastructure and supporting services, including physical access security, power connectivity and generators, HVAC systems, communications connectivity access and safety systems such as fire suppression.

Infrastructure – Hardware, firmware, software, and networks, provided to develop, test, deliver, monitor, manage, and support IT services which are not included under Platform and Application.

Platform – Computing server software components including operating system (OS), middleware (e.g., Java runtime, .NET runtime, integration, etc.), database and other services to host applications.

Application – Software programs which provide functionality for end user and Contractor services.

Storage – Physical data storage devices, usually implemented using virtual partitioning, which store software and data for IT system operations.

Backup – Storage and services that provide online and offline redundant copies of software and data.

Development - Process of creating, testing and maintaining software components.

Component Matrix	Identify contract components with contractor and/or subcontractor name(s), if applicable
Facilities	Microsoft Azure Government cloud
Infrastructure	Microsoft Azure Government cloud
Platform	Microsoft Azure Government cloud, Azure Bastion, Cloudflare, FortiGate
Application	RegSys
Storage	Microsoft Azure Government cloud
Backup	Microsoft Azure Government cloud
Development	ISC

Contractor will configure and provide the RegSys software system for SOM. The software will reside in Azure cloud.

The Contractor will require the appropriate State data for the purposes of enabling the UCC system.

5. ADA COMPLIANCE

The State is required to comply with the Americans with Disabilities Act of 1990 (ADA) and has adopted standards and procedures regarding accessibility requirements for websites and software applications. All websites, applications, software, and associated content and documentation provided by the Contractor as part of the Solution must comply with Level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0.

The RegSys Customer and Back Office Portal are mobile friendly, re-sizable and viewable on any screen size. The system is WCAG 2.0 Level AA compliant. A verification of conformance certification will be provided for Michigan’s UCC system pre-go-live.

The RegSys is designed with the public users in mind. Every screen in RegSys is designed to ensure it is not only easy to use but is compliant with all modern accessibility standards. User interfaces for the customer and internal user facing applications are designed to be graphically rich and easy to use.

Accessibility capabilities come with the implementation of a modern electronic registry system built upon best practices. Access is woven into the solution. Within RegSys system every screen is designed to ensure it is not only easy to use but is compliant with all modern accessibility standards. User interfaces for customer and internal user facing applications are designed to be graphically rich and easy to use.

RegSys is regularly tested to ensure that it is compliant with accessibility standards. RegSys has been and will continue to be audited to ensure that it is compliant with the WCAAG 2.0 Level AA standards. The Contractor will regularly review the RegSys portals to ensure that it maintains compliance with this and all other applicable standards.

6. USER TYPE AND CAPACITY

Type of User	Access Type	Number of Users	Number of Concurrent Users
End Users	Read/Write	21,000	10,500
Authorized Users	Read/Write/Admin	20	20

Contractor Solution must meet the expected number of concurrent Users. Contractors must be able to scale up or down without affecting performance.

RegSys is designed and built to address the availability, scalability, and performance needs of high-volume registry.

The Contractor solution supports variability of registry transactions, as volumes are never evenly distributed across any given day, month, or year. The Contractor solution

will be scalable to support the peaks while the business intelligence processes will help the State of Michigan anticipate and prepare for peaks.

The Contractor hosted system will be deployed to the Microsoft Azure cloud platform. The Contractor system architecture leverages the many services available such as automatic scaling to increase system capacity when user demand increases. RegSys utilizes a modern technology stack and leverages asynchronous programming where required, which increases the capacity of the product to handle high user loads.

The Contractor will utilize Microsoft Application Insights to monitor performance, including for one high volume registry implementation where the Contractor can monitor average response times across the system and proactively address any services that are not performing as expected.

The UCC system infrastructure will be optimally configured to meet the requirements of the registry. The Contractor will be running periodic performance and load tests, scaled to the requirements of the project. It is also critical to ensure post-implementation protocols with respect to security and backup policies are adhered to.

Availability includes security protection. The Contractor security includes using a best-in-class security information event management (SIEM) solution along with an experienced security team to monitor the hosting environment 7/24/365 by logging and analyzing security events. The infrastructure will contain firewalls, routers, load balancers and web, application, file and database servers necessary to support a high availability, fault tolerant RegSys implementation. The entire system will also be hosted behind Cloudflare, which is an industry leading Web Application Firewall (“WAF”). This service also provides Denial of Service (“DdoS”) protection to ensure the system is not vulnerable to denial-of-service attacks.

The Contractor’s cloud team will provide external monitoring of the software in support of an available and operational system. These checks run continuously to ensure the service is running. If there is an outage, the cloud team is immediately notified. These monitoring tools are used to provide monthly and quarterly uptime reports for the system.

In preparation for beginning the UCC services, a series of load tests will be conducted to ensure the system meets required performance metrics. The Contractor uses industry standard, automated tools, such as JMeter and K6, to perform these tests. The Contractor will work with the Supervisory Authority to determine the performance metrics. The metrics will also factor in expected traffic from potential ancillary services. Once these metrics have been established, the implementation team will create automated load and stress test scripts. The tools that the Contractor will utilize allow for

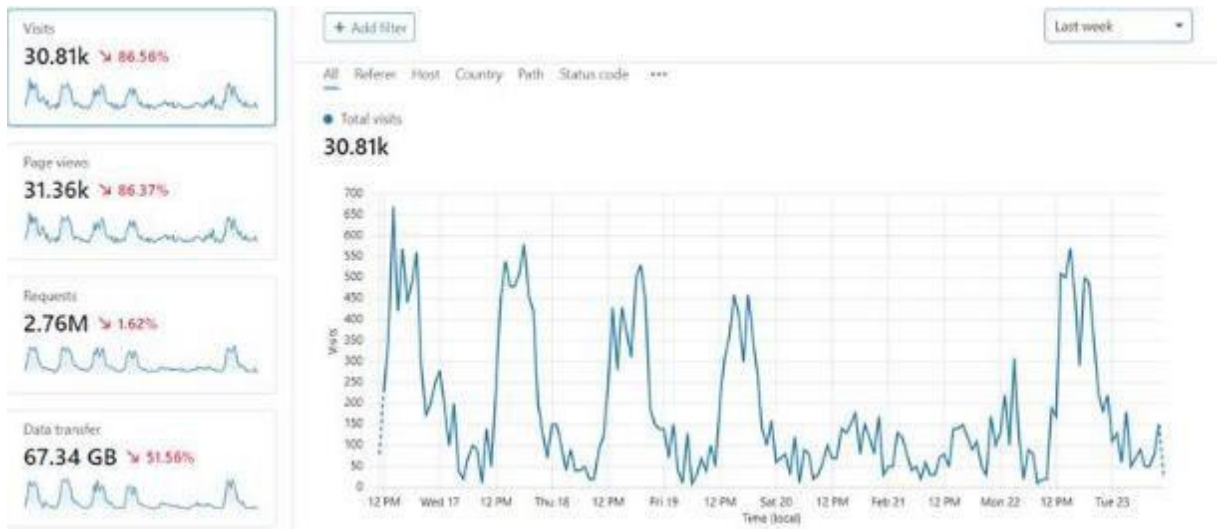
high-volume usage to be simulated and ramped up and down to test load, and to stress the capacity of the system.

A series of load tests will be conducted to ensure the system meets required performance metrics. The Contractor will use industry standard, automated tools, such as JMeter and K6, to perform these tests. The Contractor will work with SOM to determine the performance metrics. The metrics will also factor in expected traffic for all other services. Once these metrics have been established, the implementation team will create automated load and stress test scripts. The tools that the Contractor utilize allow for high-volume usage to be simulated and ramped up and down to test load, and to stress the capacity of the system as illustrated in the following sample output.



RegSys utilizes a modern technology stack and leverages asynchronous programming where required, which increases the capacity of the product to handle high user loads. The Contractor will utilize Microsoft App Insights to monitor performance in a high-volume registry and are maintaining an average response time of approximately 250ms, across all server requests.

Cloudflare, specific to the cloud hosting, is a content delivery network which acts as a middle layer between the State website and users browsing the State site. This enables content to be served up faster, speed up the State site and reduce latency. Cloudflare also has security measures built into every layer and protects the State website from attack, SQL injection, data breaches, and malicious bots. Cloudflare has a built in WAF (web application firewall) which allows the Contractor to configure the RegSys application to stop typical threats posed to Michigan’s registries.



7. ACCESS CONTROL AND AUTHENTICATION

The Contractor’s solution must integrate with the State’s IT Identity and Access Management (IAM) environment as described in the State of Michigan Digital Strategy ([1340.00.020.08 Enterprise Identity and Access Management Services Standard \(michigan.gov\)](#)), which consist of:

7.1 MILogin/Michigan Identity, Credential, and Access Management (MICAM). An enterprise single sign-on and identity management solution based on IBM’s Identity and Access Management products including, IBM Security Identity Manager (ISIM), IBM Security Access Manager for Web (ISAM), IBM Tivoli Federated Identity Manager (TFIM), IBM Security Access Manager for Mobile (ISAMM), and IBM DataPower, which enables the State to establish, manage, and authenticate user identities for the State’s Information Technology (IT) systems.

7.2 MILogin Identity Federation. Allows federated single sign-on (SSO) for business partners, as well as citizen-based applications.

7.3 MILogin Multi Factor Authentication (MFA, based on system data classification requirements). Required for those applications where data classification is Confidential and Restricted as defined by the 1340.00 Michigan Information Technology Information Security Policy (i.e. the proposed solution must comply with PHI, PCI, CJIS, IRS, and other standards).

7.4 MILogin Identity Proofing Services (based on system data classification requirements). A system that verifies individual’s identities before the State allows access to its IT system. This service is based on “life history” or transaction

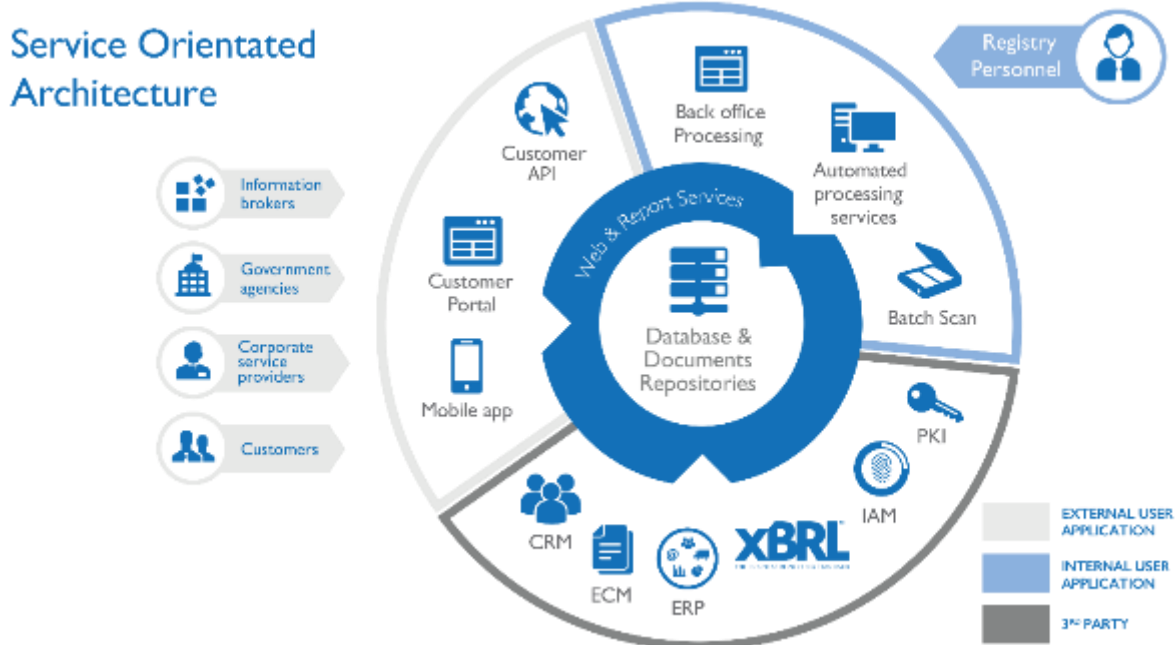
information aggregated from public and proprietary data sources. A leading credit bureau provides this service.

To integrate with the SOM MiLogin solution, the Contractor’s solution must support SAML, or OAuth or OpenID interfaces for the SSO purposes.

RegSys separates the security of internal and external users and leverages a privileged based system to control user access. The RegSys system will be configured to work with Michigan’s IT Identity and Access Management (IAM) environment. During implementation Phase RegSys will be customized and configured to integrate with the MICAM and the MiLogin solutions using SAML/OAuth/OpenID interface(s).

RegSys will provide for integration to authentication services for online users and configuration of active directory to enable role based secure access to the back-office processing application.

Authentication, authorization, and business rule validation is built into the RegSys product Service Oriented Architecture foundation to ensure the register is secure and data integrity is maintained. All activity is fully logged at the web service layer so at any time the registry can identify how the current details for a registered entity came to be and view the user and customer actions. A REST based web API will be provided for customers wishing to interface their system with all exposed customer search and filing services.



RegSys will provide for configurable, task-based workflows to be maintained across all processes. Work items are classed as tasks and are made available to sections as per configured access levels, i.e., if a particular task is to be carried out by specific groups of users, then the users would be required to have particular roles for those tasks, to be made available (for pulling). Available tasks are configured with pre-defined priorities and can be ordered in terms of date. RegSys allow tasks to be configured per process/sub-process and down to type level, e.g., submission case type. Task configuration provides management with the ability to build and maintain workflows pertinent to their business needs. Users are presented with a set of tasks as per the configuration. The tasks are presented in the same manner across all processes; whether users are processing applications, cases, orders, or correspondence to facilitate intuitive processing. All tasks can be configured to be picked up by the RegSys Auto-Processor, this provides for automated and straight-through processing to be configured as per requirements.

Authenticated users can access services. Customers are presented with a dashboard which provides for quick access to high volume services, fast search across all registers to view and/or update entity information.

The customer module in RegSys allows users to enroll as a specific type of customer, e.g., general, agent, government agency, etc. RegSys facilitates authentication services, as required. Customers can maintain groups of users under their account and can utilize draw-down account payment services.

Role based access applies to internal users.

All the above will be conducted in compliance with Michigan's policies, standards and procedures.

8. DATA RETENTION AND REMOVAL

The State will need to retain all data for the entire length of the Contract unless otherwise directed by the State.

The State will need the ability to delete data, even data that may be stored off-line or in backups.

The State will need to retrieve data, even data that may be stored off-line or in backups.

The Contractor will use an Information Governance Program which includes an Information Governance Framework and associated management policies. The framework recognizes that "Registry Records" fall under the authority of the State and are subject to the State's Registry Records Retention Schedule.

During the definition phase of the project, the Contractor will bring its registry operations records experts together with the State team to develop and define all the necessary retention schedules, procedures and processes related to records management to ensure alignment.

RegSys has a built-in 'Document Management' module which provides for the capture, storage and retrieval of documents associated with filings, correspondence, and the other aspects of the system. Paper documents can be batch scanned using the Regsys 'Batch Scan' application. Documents generated by the system or uploaded by customers online are also stored through this module. Record management business rules will be implemented as determined in the definition phase.

The documents are stored and indexed, typically on a file system, but RegSys can also be configured to store documents on the database. Documents can be searched by searching the associated item (e.g., filing, case, etc.) and easily opened and viewed.

As a scalable solution RegSys can expand data storage as needed to address SOM needs.

9. END USER AND IT OPERATING ENVIRONMENT

The SOM IT environment includes X86 VMware, IBM Power VM, MS Azure/Hyper-V and Oracle VM, with supporting platforms, enterprise storage, monitoring, and management running in house and in cloud hosting providers.

Contractor must accommodate the latest browser versions (including mobile browsers) as well as some pre-existing browsers. To ensure that users with older browsers are still able to access online services, applications must, at a minimum, display and function correctly in standards-compliant browsers and the state standard browser without the use of special plugins or extensions. The rules used to base the minimum browser requirements include:

- Over 2% of desktop and mobile & tablet site traffic, measured using Michigan.gov sessions statistics and
- The current browser identified and approved as the State of Michigan standard

This information can be found at <https://www.michigan.gov/browserstats>. Please use the most recent calendar quarter to determine browser statistics. Support is required for those desktop and mobile & tablet browsers identified as having over 2% of site traffic, the current browser version as well as the previous two major versions must be supported.

Contractor must support the current and future State standard environment at no additional cost to the State.

RegSys is designed to be vertically and horizontally scalable and very flexible in terms of deployment options. The various components can all be installed on a single server or split across multiple servers. Individual components can be deployed on multiple servers where redundancy, high availability and load balancing are required.

The Contractor will meet the browser version as part of this Contract.

The Contractor will use stringent care and security provisions to implement and support RegSys. To enable the rapid and cost-effective implementation of RegSys as contracted, the Contractor will use resources in Canada. The Contractor team working on the implementation and support will comply with all State PSPs.

Work would be done in a restrictive and secure process where the data never leaves the continental USA and cannot be downloaded. For selected the Contractor employees to access data for the purposes of supporting the implementation they would go into a USA based virtual machine to indirectly access the data. All data related activity would take place only within that environment. This activity would be governed by The Contractor's corporate requirements for data handling and security. Access to the cloud environment would be managed via the Azure Bastion service. Bastion is a platform-as-a-service facility provided by Azure that resides inside the Azure virtual network and allow users to log into virtual machines. The bastion service does not allow data to be copied out of the remote session via system clipboards. Bastion is accessed via the azure web portal. Users would log into the azure portal and use bastion to open a connection to the virtual required machine. This machine will be in the USA. Through the clipboard restrictions and use of firewall policies the Contractor will prevent data from leaving the "Virtual Data Center" that resides in the continental USA.

The Contractor will follow current SOM IT environment includes X86 VMware, IBM Power VM, MS Azure/Hyper-V and Oracle VM with supporting platforms, enterprise storage monitoring and management running in house and in cloud hosting providers.

RegSys is a complete registry system and directly enables the operational requirements for performing transactions.

To support required interfaces to external systems, RegSys has been developed on the API First' principle which allows for services to be made available for external customers, agencies, and third-party systems to seamlessly integrate to as required.

The RegSys relationship with the broader SOM IT environment would be interface driven. There is a set of APIs made available by the product that provide the services of

the registry. The RegSys customer portal uses these APIs to provide the interface for the users. The APIs can also be made available to third parties (including access points for jurisdictions) as required. This provides the ability for different systems to consume the UCC services as permitted.

While RegSys comes with significant core capabilities, functionality, and “built-in” best-practices, it also provides the flexibility and configuration capabilities to optimize its fit within the SOM environment. As a result, RegSys will continue to co-exist over time with the evolving SOM IT environment.

The RegSys product will be continually upgraded with new and improved functionality. These enhancements are made available to license holders. Product updates of a critical nature are made available for implementation immediately. Minor product upgrades are typically made available every quarter with major upgrades on an annual basis.

The Contractor will be dedicated to maintaining the RegSys implementation at an operational level that meets the requirements of this Contract.

Maintenance releases and product updates are included as part of the RegSys licensing agreement. Changes to the system will be made only with SOM approval. If the State does not keep RegSys current, i.e., by not implementing maintenance releases and updates resulting in the RegSys application being one major release behind, the State acknowledges that the Contractor may incur more effort and risk in implementing future releases and product updates that is not reflected in the Maintenance & Support costs set out in Schedule B. In such case, the Contractor will request that the State submit a Change Request as set out in section 2.2 of the Contract, and the State shall comply.

Customizations specific to Michigan’s implementation will be accommodated through a change request process, described in the next section.

The Contractor will assign a Canadian based Account Manager responsible for the relationship including the ongoing service and support of the Michigan account. Discussions and updates regarding new releases of RegSys and evolution of the product roadmap will be part of the regular contact between the State and Account Manager. The Account Manager will also be a key coordination point for any customizations requested by SOM.

Changes to the system may be required by the State. These will be addressed through the State’s change request process.

All updates will be tested by the Contractor project QA team in accordance with Contractor QA testing processes. These tests are designed to test the complete system

with all of the functional requirements completed. Once these tests have been completed, the system will move into User Acceptance Testing (UAT). During this phase SOM will test the system updates to ensure they execute properly. When UAT has completed, SOM will provide UAT sign-off and approval to deploy the changes into the production environment.

There are no required plug-ins for RegSys to meet the system requirements.

10. SOFTWARE

Software requirements are identified in **Schedule A – Table 1 Business Specification Worksheet**.

Contractor must provide a list of any third party components, and open source components included with or used in connection with the deliverables defined within this Contract. This information must be provided to the State on a quarterly basis and/or if a new third party or open source component is used in the performance of this Contract.

Look and Feel Standards

All software items provided by the Contractor must adhere to the State of Michigan Application/Site standards which can be found at <https://www.michigan.gov/standards>.

Mobile Responsiveness

The Software must utilize responsive design practices to ensure the application is accessible using (including but not limited to) a computer, mobile phone, or tablet. This refers to a mobile browser, not a mobile application.

SOM IT Environment Access

Contractor must access State environments using one or more of the following methods:

- State provided VDI (Virtual Desktop Infrastructure) where compliant.
- State provided and managed workstation device.
- Contractor owned and managed workstation maintained to all State policies and standards.
- Contractor required interface with State systems which must be maintained in compliance with State policies and standards as set forth in **Schedule E – Data Security Requirements**.
- From locations within the United States, jurisdiction territories and Canada.

RegSys is an end-to-end solution, with a suite of configurable components. It can support multiple registers on one platform developed upon cutting edge technology. RegSys does not require integration to other third-party services or systems to support the operational requirements of a registry. It has been developed on the 'API First'

principle which allows for services to be made available for external customers, agencies, and third-party systems to seamlessly integrate to as required (e.g., MS CRM).

RegSys is built upon the following foundation and capabilities:

- Its architecture allows it to scale up and down based on demand.
- RegSys uses Microsoft SQL Server as its database.
- RegSys provides the ability to have an unlimited number of individual assets in a single transaction.
- RegSys provides the ability to fully automate transactions as they are submitted.
- The RegSys customer portal is fully responsive and accessible. This means it can be accessed on a desktop, tablet or phone and is usable by the visually impaired.
- RegSys is compatible with all modern internet browsers.
- RegSys has been built with an API first approach.
- RegSys contains a configurable forms engine.
- The forms engine also provides the ability to specify business rules that must be met.
- RegSys will provide an extensive user verification platform to manage access to the registry.
- RegSys has multiple options related to digital signatures ranging from a simple electronic signature through to full Qualified Electronic Signatures (“QES”).
- RegSys provides a search module that will allow users to search for registrations from the customer portal.
- RegSys provides internal auditing that tracks all changes to data in the system.
- RegSys utilizes SQL Server Reporting Services and PowerBI to provide standard reporting and advanced business intelligence capabilities.

From a functional perspective RegSys is centered around the core trusted registry principles of submission, enquiry and enforcement.

RegSys provides for the full enquiry lifecycle including fast searching functionality, advanced search functionality, document and report ordering, shopping cart functionality,

delivery and custom dispatch methods, fee collection and order fulfilment & workflow functions.

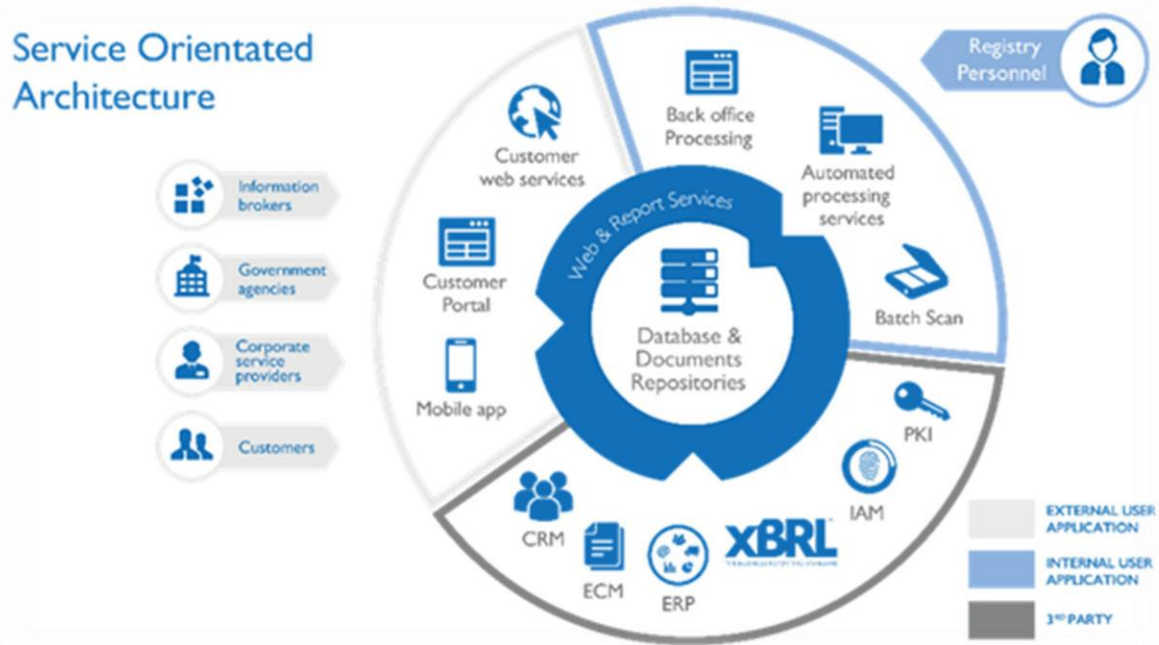
The following “User Interfaces and Modules” illustration shows the primary user interfaces, the public facing ‘Customer Portal’ (“CP”) and the ‘Back-Office Processing Application’ (“BO”). CP is fully responsive on all devices and is developed on the Angular web framework, which provides for a rich User Experience (UX) to be enabled, providing “app- like” functionality. The RegSys Customer Portal User Interface can be configured to meet specific user interface requirements, including branding. The BO application in RegSys facilitates a range of self-service features allowing back-office users to perform processing, maintenance, and administrative functions relevant to their role. Users are presented with a customizable dashboard which allows the user to manage their work in an orderly manner.

RegSys’ suite of components, shown in the bottom half of the “User Interfaces and Modules” graphic, are configurable to the requirements of Michigan.



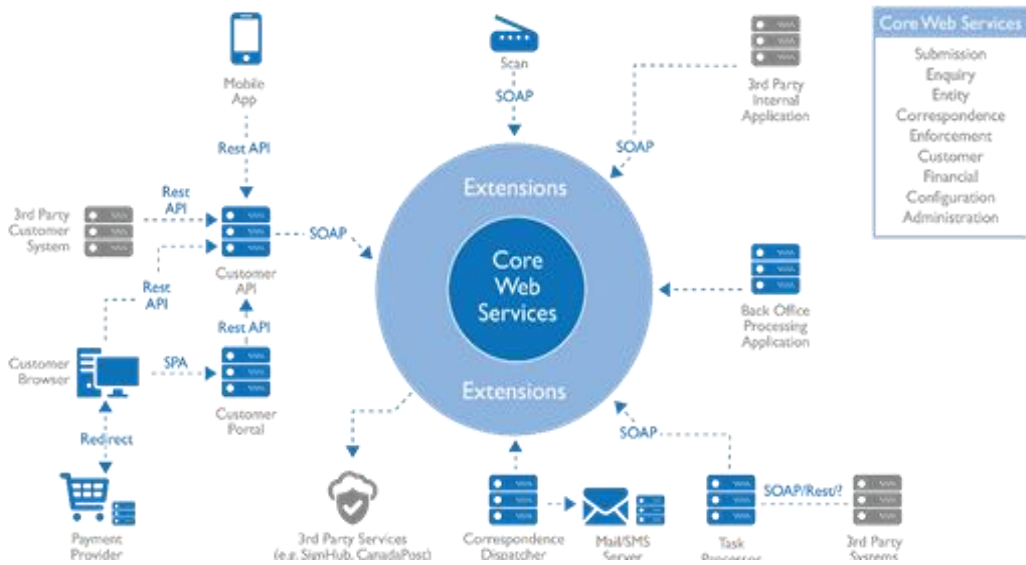
RegSys enables a consistent user experience and ease of use. The RegSys Customer Portal is a modern, intuitive browser-based interface that is fully responsive, mobile friendly, re-sizable, viewable on any screen size and WCAG 2.0 Level AA compliant.

RegSys is built entirely on an MS.NET platform with SQL server as the database. RegSys provides a complete range of integrated components based on a modern, service-oriented architecture leveraging open, web-based standards such as RESTful services, XML and JSON payloads and facilitates SSL/TLS secured communications.



RegSys – Technical Overview

Architecturally all functionality is provided through a single set of web services that all applications must use to access and update data in the register or perform other related tasks. Authentication, authorization, and business rule validation is built into this layer to ensure the register is secure and data integrity is maintained. All activity is also fully logged at the web service layer so at any time a registry can identify how the current details for a registered entity came to be and view user and customer actions. A REST base web API is also provided for customers wishing to interface their system with all exposed customer search and filing services.



RegSys – Architecture

The following table outlines the standard components within in RegSys:

Component	Type	Purpose
Core		
RegSys Database	SQL Server Database	Store all relational data for the system and text indexes names.
RegSys Web Services	.NET Windows WCF Service	Core RegSys web services used by all RegSys applications.
Applications		
RegSys Customer Portal	Angular Web Application	Used by customers to file submissions and order information. Uses the Customer Portal API.
RegSys Customer Portal API	ASP.NET Web API Application	Used by the RegSys Customer Portal and 3 rd party systems to access search and filing services.
RegSys Back Office Processing Application	ASP.NET MVC Web Application	Core application used by internal staff to perform their work.

RegSys Batch Scan	NET Window Forms Application	Batch scanning of paper documents.
RegSys Customer API	ASP.NET MVC Web API	Used by customer systems to file submissions and order information (M2M).
Automated Processing Services (can be added to)		
RegSys Correspondence Dispatcher	.NET Windows Service	Dispatches any correspondence marked for dispatch via email, print, fax, or any other required channels.
RegSys Task Processor	.NET Windows Service	Processes tasks related to submissions, inquiries, and cases.
RegSys Watched Entity Processor	.NET Windows Service	Create correspondence notices for customers watching entities that have had activity.
RegSys Enforcement Processor	.NET Console application scheduled to run nightly	Handle various bulk enforcement scenarios such as annual return

As a comprehensive solution, RegSys is able to fulfill Michigan’s requirements. Other than configuration and some customization outlined in Table A, there are no additional unique software requirements contemplated as part of this response.

All service and support for the State of Michigan would come from Canadian operations and resources. The Contractor will align with State of Michigan’s data handling requirements and State data will not leave the USA. This is described in detail in the “State System Access Requirements” section within “9. End User and IT Operating Environment”.

The Contractor does not anticipate any custom software required to support internal SOM systems. Given it’s API centric design, the RegSys product is able to interface with State of Michigan’s systems.

The Contractor is offering Michigan a Perpetual Sublicense for RegSys.

The Contractor will leverage open-source tools and frameworks as part of its RegSys solution. RegSys is developed utilizing the .NET and Angular frameworks.

Open Source Tools
<p style="text-align: center;">Microsoft.NET</p> <p>Autofac AutoMapper BCrypt Castle Core CsvHelper dotless FluentValidation Foolproof GreenPipes Hashids.net (Hash IDs .NET) HtmlSanitizer Humanizer jQuery JsonApiSerializer MassTransit Nager.Date nClam Newtonsoft.Json NLog Polly QRCoder ReportViewer for MVC SimMetrics StackExchange.Redis Stateless Swashbuckle.AspNetCore TinyMCE Xunit</p>
<p style="text-align: center;">Angular (latest version v14)</p> <p>Auth0Jwt Bootstrap CoreJs FileSaver FontAwesome</p>

HammerJs IntlTelInput Lodash Mime Moment NgRx Rxjs TextMaskAddons TsHelpers TsLib WebAnimations.Js Zone.Js
Developer Tools
Visual Studio Professional
SQL Server Management Studio

The RegSys Customer is a modern, intuitive browser-based interface that is fully responsive, mobile friendly, re-sizable, viewable on any screen size and are WCAG 2.0 Level AA compliant.

The RegSys customer portal is fully responsive and accessible. This means it can be accessed on a desktop, tablet or phone and is usable by the visually impaired. RegSys is compatible with all modern internet browsers.

11. INTEGRATION

Contractor must integrate their solution to the following technologies:

Current Technology	MiLogin – the State supports the following types of authentications: <ul style="list-style-type: none"> • HTTP Header • Federation Technology • SAML • OAUTH • Other
Volume of Data	Approximately 21,000 users
Format of the input & export files	NA

Current Technology	CEPAS redirect
Volume of Data	Approximately 86 per day
Format of the input & export files	NA

Current Technology	FileNet - API
Volume of Data	FileNet Storage May 2022 231filenetmdoosucc2es.pea – 703gb
Format of the input & export files	Input - DLL – API client, Export - .pdf

Current Technology	CARS - API
Volume of Data	Approximately 232 per day
Format of the input & export files	NA

The Software will integrate with FileNet 5.5.10 and Contractor will maintain integration, at no additional cost, with any updated versions of FileNet the State may deploy.

The Contractor must make sure all connections to required systems will be done via a Public Rest API. This API comes standard with RegSys and will provide the ability for

different systems to connect with the UCC system. The API is designed using modern development techniques and is well documented, allowing for external parties to more easily integrate with it.

During the implementation phase of the RPM project all the required integrations will be developed. ISC will then perform a set of end-to-end system tests to check those custom integrations with Michigan’s external systems.

RegSys was developed on the ‘API First’ principle which allows for services to be made available for external customers, agencies, and third-party systems to seamlessly integrate to, where required. It supports multiple channels, including paper-based services, in addition to facilitating and enabling high levels of automation and straight-through processing.

RegSys provides for seamless integration to third party applications, given the API first nature of all services, as well as built-in workflow and case management capabilities, which are further described below.

RegSys will integrate with Michigan’s choice of FileNet.

12. MIGRATION

Contractor must migrate the data identified in the table below:

Current Technology	SQL 2016, .NET 4.8, MVC
Data Format relative to the database technology used.	Stored in a Relational Database
Number of data fields to give Contractor awareness of the size of the schema.	35 fields on the UCCFiling table
Number of Records	2,895,554 records
Database current size	100 GB
Data quality	Serious concerns about data integrity
Data Cleaning	May require data cleansing and standardization

The Contractor will migrate the registry data to the RegSys and will involve the migration of structured (relational data) and unstructured data (documents).

- Structured data is stored in a database and includes all the core records maintained over each registered entity’s life cycle. Additional data such as notes, correspondence, and annual filing information, may also need to be migrated. User profiles may also need to be migrated.
- Unstructured data includes all forms and documents received. These forms and documents may have been scanned from paper, uploaded electronically, or generated electronically by the registry. It may also include additional correspondence received or sent to an entity and certificates issued by the registry. Some documents may also exist in paper format only or in older archive formats such as microfiche.

The Contractor will migrate the data from the legacy system as early as possible in the implementation phase to provide the Registry staff with a view of the data in the new system. This view is often more intuitive for operators than exported data tables allowing the Registry staff to better identify potential data integrity issues. This activity involves iteratively developing, refining, and testing the data migration routines, and continues throughout the implementation phase. Migrated data is made available iteratively to provide the other development activities with real migrated data.

Data Migration Approach

Phase	Description
Planning (ISC)	<p>The existing source data is examined and analyzed, and any data quality issues are identified early and will be explored further with the Registry staff to determine the best course of action to correct, i.e., before, during or after migration.</p> <p>A certain amount of automated cleansing during migration is usually feasible but sometimes corrective action may need to be taken on existing systems before migration or the system needs to provide support for cleansing data after migration.</p>

<p>Planning (ISC & SOM)</p>	<p>The development of a data migration (conversion) plan is designed and documented in terms of:</p> <ul style="list-style-type: none"> ▪ Roles & Responsibilities (including SOM) ▪ Collaboration Procedures (enabled through Azure DevOps and Teams) ▪ Test Plan to show migrated data will be verified against the source data e.g., reports comparing source and target data outputting summary results. ▪ Logical groupings (models) of source data, for each source table and related statistics (number of rows etc.) ▪ Mapping - source data to be migrated and its target destination, e.g., source table & field -> target table & field, and the effort assessment. ▪ The plan will clearly identify the timing of migration of each logical grouping. ▪ Data Migration process (e.g., database to database, extract-transform-load etc.) and any transformations to be applied during migration <p>The impact of the cleansing and/or transformation will be identified in terms of time and effort.</p>
<p>Execution Phase</p>	<p>The data migration and verification programs are developed and executed iteratively in line with the overall agile approach to implementation, allowing for relevant data to be made available to the implementation team. It also provides for ongoing testing of the migration. This data migration process is incorporated into the overall Transition Plan.</p> <ul style="list-style-type: none"> ▪ An exact copy of the source database will be created on the target environment. ▪ Historical transactional data will not be migrated unless it is classed as 'register data'. ▪ Data anomalies that are identified will be documented.

The plan will be completed with the overall implementation of RegSys in twelve months, the Contractor will need to focus on the data to migrate into RegSys. The Contractor will work with the State to identify which data needs to be migrated into RegSys, and which data will be archived. Archiving some legacy financial, workflow and event history type data has always proven to be a time saver because data such as this is often very specific to the legacy system and can be both intensive and time consuming to integrate into RegSys

because additional screens and reports are required to support the viewing of that data. To address this potentially lower-value data, previous clients have migrated this type of legacy data into a SQL Server database where the data could be queried as required.

The initial phase '**Planning (ISC)**' phase involves getting a complete copy of the current data model and performing a study of the data model to gain an understanding of the data.

If SOM has any additional input, such as their own plans, suggestions, or insight into the data, especially if there are plans to cleanse or transform the data, this input is most welcome and will be included as part of the initial study process.

The initial Data Migration Plan is the input to the '**Planning (ISC & SOM) phase**'. The Logical Grouping of the data will help quantify the effort and work required by both parties and will help to identify the time required to complete the migration.

If the plans for data cleansing or data transformation are provided at this stage then they can be included in the plan and the plan updated to include the time, effort and risks involved.

The plan for the migration of documents must also be developed at this stage, especially if documents need to be converted e.g., from tiff to pdf.

The '**Execution phase**' begins when the Planning Phase by the Contractor and SOM has provided enough to start with, this is an agile and iterative approach so the more that can be confirmed at the planning phases, the better the execution phase will be.

The migration will be performed using Microsoft products such as SQL Server Integration Services (SSIS) and C# code which are utilized using Microsoft Visual Studio, SQL Server T-SQL code which is implemented using SQL Server Management Studio. PowerShell will be used for batching programs and program control. Data cleansing and data transformation will be included within each iteration of the data migration process where the results will be immediately available for use in the application and available for testing and further review and refinement if necessary.

All migrations will be performed in a development environment, the Legacy System will not be updated or impacted on, in any way.

The data migration test plan will provide for testing to be completed at the end of each iteration. The data that has been migrated in each iteration, will be tested by the migration team, and will also be tested as part of the overall implementation. Data issues are logged and recorded to the backlog and incorporated into the next iteration, as required.

During testing the Contractor and State will identify what is failing and decide how best to correct it. The failure may be the application, the data or a combination of both application and data. Efficient decision making by both parties in identifying the best way to correct the problem is crucial to ensure the project stays on schedule.

The State will provide testers who are confident to test the logical grouping associated with their workload that would be the most effective. (For example, UCC data is tested by those who manage UCC filings, payment data is tested by those in finance/accounts, etc.) The retrieval of documents must also be included in testing to ensure that documents are retrieved as efficiently as possible and are correctly presented.

Azure Dev Ops will be used to control the migration project and all stages of the project are documented using Dev Ops, this includes Test Plans and the Outcome of Testing. All members of the team have access to Dev Ops.

Within the Data Migration effort, any failures or problems identified during an iteration in the execution phase are identified and used as input to the next iteration.

The data migration plan and associated procedures will provide for a full copy of the source database to be created on the target environment. This database will be included in backup routines, to allow for recovery, retention, and business continuity processes.

After go-live, reports and queries can be developed/run against this database, on request, where required. The retention policy with respect to this database can be agreed with SOM. Access to all databases and repositories adhere to strict access and security protocols.

The legacy system is not changed in any way by the migration process. Regular backups from the Legacy system are all that is required as the base for the migration process.

Once the RegSys database and application are ready, the transition to RegSys can occur, thereby leaving the legacy system intact and available if required.

When the data migration process is accurate and complete, the final task is to perform the final migration into the RegSys production database. Throughout each iteration, the data migration will be timed so that the Contractor will have an accurate estimate on how long the final migration will take.

The Data migration plan and related procedures will include reports on the results of each iteration of the migration, including the final migration. The final SOM-approved report will detail the results of the implementation process. It will include the results of data migration, summary of the go live activities and the status of the now live system. Observations and lessons learned from the go live event will also be reported on.

Additionally, the final Michigan approved report will be complete detailing the various logical groupings of data that were to be migrated along with results showing details of the successful migration. All data transformations and cleansing details will be included.

The report will clearly show the logical groupings and the numbers involved in the migration process and will display correlation between the expected migration and the actual migration.

The UCC Registry system will be optimized to meet the current and future requirements of the registry. This will be achieved by running periodic performance and load tests, scaled to the requirements of the project. It is also critical to ensure post-implementation protocols with respect to security and backup policies are adhered to.

The Contactor software, services and interfaces will enable millions of search and registration transactions daily.

- The Contractor will utilize Microsoft Application Insights to monitor performance, including for one high-volume registry implementation where the Contractor can monitor average response times across system and proactively address any services that are not performing.

In preparation for going live with the registry services, a series of load tests will be conducted to ensure the system meets required performance metrics. The Contractor will use industry standard, automated tools, such as JMeter and K6, to perform tests. The Contractor will work with the State to determine the performance metrics. Once the metrics have been established, the implementation team create automated load and stress test scripts. The tools the Contractor will utilize allow for high-volume usage to be simulated and ramped up and down to test load, and to stress the capacity of the system.

Data migration cost are included as part of this Contract.

The RegSys implementation team will develop a data migration plan. The data migration plan will incorporate five distinct phases – analyze, design, develop, test and conduct.

13. TRAINING SERVICES

The Contractor must provide administration and end-user training for implementation, go-live support, and transition to customer self-sufficiency.

Contractor must develop and submit for State approval complete, accurate, and timely documentation/training materials (including, but not limited to, video/audio training

videos and public communications) and will update any discrepancies, or errors through the life of the contract without any additional charge to the State.

The training provided by the Contractor must include the following, as appropriate by MDOS and DTMB:

- Introductory training for core team if a proprietary platform or project management tools will be used.
- Core team developer training as appropriate
- Report development training
- User Acceptance Testing (UAT) team training prior to UAT
- SOM User training prior to Go-Live
- System Administrator training
- Post Go-Live Developer and Maintenance training as appropriate

The Contractor must work with the State to develop a Training Plan that contains the following, but is not exclusive to:

- Identifies all training materials
- Identifies scope and objectives of training
- Identifies roles and responsibilities of users
- Clarifies evaluation practices for determining if learning outcomes are achieved
- Addresses training strategy
- Identifies required training resources, locations, and environments
- Identifies training dates and times
- Specifies who will attend each section of training

State will have ownership of all training materials developed.

The RegSys training program will cover all stakeholder groups, i.e., internal staff and external end-users. The primary purpose of the training program is to ensure that each set of users is aware and capable of utilizing all functionality that is available in the system. Given the different functionality that is required for each of the user types, the RegSys training program is divided into two distinct groupings.

External End-Users

External users are those that use the Customer Portal to search and register UCC and related filings. Users, particularly external customers, expect applications to be intuitive and have a preference for individual, self-directed learning. As such, the training program for external users will focus on supporting customers through built-in help

materials within the Customer Portal application. This help content will be designed to cater for users of all technical capability.

The Customer Portal will be built specifically to empower users to interact with and have access to the system at their convenience. The Customer Portal has a configurable field level help model which enables the user to identify the details required at each step of the process. The Customer Portal also provides configurable “Filing / Process Level” instructions that helps the user to understand what is required to successfully complete the desired task. This can be defined and refined to each business process, to ensure users get the most accurate help available.

In support of the larger change management plan, the Contractor will be developing a specific on-boarding program designed to guide the user through the initial stages of their interaction with the solution. This introductory onboarding program will prioritize:

1. Customer awareness of the new solution and the benefits it will provide.
2. An overview of the workflow and how core functions of the solution operate.
3. Providing a clear set of activities necessary to successfully onboard to the new solution (e.g., user registration and account set-up.)
4. Offering of support options available to customers – in-application, online and offline.

The training methodology provides for inclusive and interactive engagement between all members of the project team, including relevant stakeholders, throughout the lifecycle of the project and beyond. The Contractor will advise the project team on the delivery of a Change Framework and Change Management Policy as defined in Project Management, Planning & Business Analysis Requirements section.

The users will be working with the Contractor implementation team from the initial requirements gathering and design through the implementation phase, where users will be configuring the system, e.g. building forms, alongside the Contractor implementation team.

Internal Staff Users

Internal users are required to have an in-depth understanding of both the Customer Portal and the internal Back Office Processing Application. To ensure that staff can support external customers in using the Customer Portal, the Contractor team will collaborate with SOM staff to detail the typical types of problems that external users may experience when submitting filings, as well as how to manage them.

The training program will train internal users how to explain the problems and solutions to the customers. The internal user will be trained to provide customer support and

service. Training will be conducted with RegSys subject matter experts on specific modules of RegSys functionality. Each internal user will have access to the sandbox environment to get a hands-on feel for each area helping them become “super users” and learning training/presentation techniques for internal training sessions.

The RegSys training program will provide detailed documentation and manuals with descriptions of everything that is covered in the training program. The manuals will be available to download at an application level. Refresher training is also available, at the request of the State.

RegSys provides a quick setup wizard for internal State users. This quick setup wizard appears the first time those users login to the RegSys. The quick setup wizard enables users to complete an initial dashboard configuration for features that they will regularly use.

RegSys provides help functionality for both the customer portal and back office users.. The help content is editable through the back office, providing help with general information or for specific submission type information. For the customer portal, help text is included for forms, which is added during the development of the forms,

It also gives users the ability to respond to areas which create user pain points by updating the help material to enable future users to overcome these issues and therefore reduce or mitigate these pain points.

Web Based/eLearning Modules

The Contractor will utilize an online environment where training courses are created, uploaded, accessed and viewed. Training courses are created for each system module in both the Customer Portal and Back Office Processing Application.

Training courses can be converted into eLearning modules, which will guide users through the process of the course. The eLearning module utilizes a SCORM |xAPI | cmi5 format.

Users are assigned to courses and progress is tracked per training course, up until course completion. This enables senior level users to track progress across all internal users. RegSys also provides online tours. Online tours are quick high-level tours around specific screens on the application. They are not detailed guides but provide an overview of the selected screen and the parts of that screen that the user / operator will need to focus.

System Administrator Training

The Contractor will provide RegSys code and technical walkthroughs to enable users to gain a thorough understanding of the solution. The Contractor will hold technical workshops with client representatives virtually. Training will include best practices in any integration technologies and activities such as data migration.

The specific training program will provide comprehensive administration training made available to the required users. This training will explain in detail the full capability of RegSys and will describe the processes that are required to make configuration changes in the system. These users will also be required to undergo the same training as ordinary internal users to ensure they too have the same detailed understanding of all functionality. A sandbox environment will be available for internal users to practice processes and get familiar with functionality throughout the life cycle of the project. This allows for a completely immersive training experience for all project members. These staff members will also receive specific report writing training classes explaining how SSRS and Power BI works, and how best to utilize the functionality for the dashboards.

RegSys will provide a training course on the configuration module of the system which system administrators can utilize. All course content is editable and configurable. Each course steps the user through the modules in the Back Office Processing Application, resulting in users understanding the configuration module of RegSys and the ability to successfully configure each system module.

Training Schedule

Throughout the project, the Contractor will provide comprehensive training and documentation to ensure that required skills and knowledge transfer take place to enable SOM to support and maintain the system in the absence of Contractor. The Contractor will fully support the State training requirements.

The Contractor will use storage location of the States choice to host the training videos in a structured approach that guides the State in the training. Users will learn RegSys and State business processes and regulations that are contained in RegSys. The Contractor will update training content in central location that will be available to the State.

14. TRANSITION RESPONSIBILITIES

Please see **Schedule G – Transition In and Out**

15. DOCUMENTATION

The Contractor must provide all documentation in a State approved electronic format and hard copies upon request of the State. Contractor must provide all user manuals, operating manuals, technical manuals, data element dictionary and any other instructions, specifications, documents or materials, in any form or media, that describe the functionality, installation, testing, operation, use, maintenance, support technical or other components, features or requirements of the Software.

The Contractor must provide the following documentation:

- All required SUITE Documentation as specified by the State of Michigan without additional cost to the State identified during project Tailoring.
 - Functional and System Design document
 - Installation plan/guide
 - Implementation plan
 - Module configuration documents sufficient for configuration maintenance purposes
 - Data Migration and Conversion Plan
 - This would include mapping of data
 - Requirements Traceability Matrix
 - Requirements Review Report
 - Business Workflow Documents
 - Development Specifications Document
 - Provide or assist with the EASA
 - Knowledge Transfer Plan
 - Test plan
 - Test results
 - Interface/Integration Technical Design Documents
 - Baseline End-User training manuals to be used as a basis for “User Manuals” and online help

The above list is not a complete list of documents. There are documents required in other sections of the document.

The Contractor must maintain all documentation and update all documentation during the term of the contract, including the warranty period, software license period and maintenance agreement. Documentation must be in alignment with the system version in test and production.

The Contractor must provide all documentation in a State-approved format that facilitates updating and allows for clearly identified revisions to the documentation.

The documentation of components, features, and use of the hardware/software must be detailed so that resolution of most problems can be determined from the documentation and most questions can be answered prior to initiation of formal support requests

The Contractor will implement RegSys under the RegSys Project Methodology. The Contractor will adhere to agile principles to implement the requirements, as set forth in this Contract. The Contractor will implement processes “application focused”, where the project teams are providing demos of functioning services and recording feedback from the business users. Azure DevOps is used to record and implement the feedback from the definition phase through to Go Live.

The Contractor will provide extensive set of supporting documentation and user manuals which will be used to provide detailed descriptions of everything covered in the training programs. The manuals will also be available for download at an application level.

16. ADDITIONAL PRODUCTS AND SERVICES

RegSys solution will include all elements of the technology stack to support the solution have been identified throughout the Contract.

17. CONTRACTOR PERSONNEL

Contractor Contract Administrator. Contractor resource who is responsible to (a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract. Contractor must inform the State in writing of any change to this resource.

Contractor	
Name	Siva Ramamoorthy
Address	Suite 300, 10 Research Drive, Regina, SK, S4S 7J7
Phone	639-560-4157
Email	Siva.Ramamoorthy@isc.ca

Contractor Security Officer. Contractor resource who is responsible to respond to State inquiries regarding the security of the Contractor’s Solution. This person must have sufficient knowledge of the security of the Contractor Solution and the authority to act on behalf of Contractor in matters pertaining thereto. Contractor must inform the State in writing of any change to this resource.

Contractor	
Name	Chris Rothecker
Address	Suite 300, 10 Research Drive, Regina, SK, S4S 7J7
Phone	306-787-5647
Email	chris.rothecker@isc.ca

18. CONTRACTOR KEY PERSONNEL

Contractor Project Manager. Contractor resource who is responsible to serve as the primary contact with regard to services who will have the authority to act on behalf of the Contractor in matters pertaining to the implementation services, matters pertaining to the receipt and processing of Support Requests and the Support Services.

Contractor	
Name	Jeremy Hall
Address	Suite 300, 10 Research Drive, Regina, SK, S4S 7J7
Phone	306-526-8413
Email	jeremy.hall@isc.ca

Contractor	
Name	Siva Ramamoorthy
Address	Suite 300, 10 Research Drive, Regina, SK, S4S 7J7
Phone	639-560-4157
Email	Siva.Ramamoorthy@isc.ca

19. CONTRACTOR PERSONNEL REQUIREMENTS

Offshore Resources. Offshore Resources are not permitted, including any Subcontractors.

20. STATE RESOURCES/RESPONSIBILITIES

The State will provide the following resources as part of the implementation and ongoing support of the Solution.

State Contract Administrator. The State Contract Administrator is the individual appointed by the State to (a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract.

State Contract Administrator	
Name	Jeremy Lyon
Phone	517-230-2858
Email	LyonJ5@michigan.gov

Program Managers. The DTMB and Agency Program Managers (or designee) will jointly approve all Deliverables and day to day activities.

DTMB Program Manager	
Name	Daniel Klodt
Phone	517-930-3506
Email	klodtd@michigan.gov

Agency Program Manager	
Name	Rayne Sherman
Phone	517-275-2862
Email	shermanr@michigan.gov

21. MEETINGS

At start of the engagement, the Contractor Project Manager must facilitate a project kick off meeting with the support from the State’s Project Manager and the identified State resources to review the approach to accomplishing the project, schedule tasks and identify related timing, and identify any risks or issues related to the planned approach. From project kick-off until final acceptance and go-live, Contractor Project Manager must facilitate weekly meetings (or more if determined necessary by the parties) to provide updates on implementation progress. Following go-live, Contractor must facilitate monthly meetings (or more or less if determined necessary by the parties) to ensure ongoing support success.

The Contractor must attend and facilitate as required by process or by the State of Michigan, the following meetings, at a location and time as identified by the state, at no additional cost to the State:

- Kick off meeting, within 30 business days from the award of contract unless otherwise specified by MDOS.

- The meeting will outline the proposed approach, including but not limited to the following: an overview of the solution, project plan, project schedule, Contractor and State resources and responsibilities, risk mitigation plan, etc. The meeting will be held in Lansing, Michigan, at a date and time mutually acceptable to the State and the Contractor
- Project planning sessions
- SUITE tailoring sessions
- Discovery/Requirements and analysis meetings
- Ongoing collaborative team meetings to facilitate discovery and development are required.
- If Agile Scrum development approach is proposed, then all Scrum ceremonies, including daily Scrum, sprint planning, sprint reviews, sprint retrospectives, backlog grooming, and artifacts will be encouraged and expected.
- All other meetings needed to successfully implement the new system.
- Daily standup/JAD sessions, depending on approach
- Security plan assessment and review sessions
- Business and technical review and validation meetings, to ensure a mutual understanding of the requirements, business workflow, business needs, and required system functionality
- Formal walkthrough and signoff meetings
- Lessons Learned after implementation and final signoff meeting

Contractor will be expected to provide lessons learned as will State of Michigan.

The Contractor must provide an agenda, specific objectives and minutes thereafter for each meeting for the life of the project. Meeting minutes must be provided within 24 hours of the meeting.

Details regarding collaboration activities are described in the Project Management section of the Contract, both within the implementation methodology process as well as within the project plan steps and milestone.

The meeting types within the project will consist of:

Meeting Type	When	Attendees	What
Steering	Bi-weekly	Project Managers, project team	Project status report
Kick-Off	Project start	Project team	Project launch
Ongoing Review	Weekly	Project team	Project progress reviews

Project Tasks	Weekly	Project members as appropriate depending on task	Input and support for design, implementation, and transition efforts as well as ancillary activities
Daily Stand-up	Daily as appropriate	Project team/Business users	Checkpoints
Special review meeting	As required	Project team/Business users	Project discussions
Wrap Up	Project end	Project Team	Confirm completion of requirements
Lessons	Project end	Project Team	Share and compile findings

The Contractor Project Manager will be responsible for managing and ensuring that the needs and any concerns are incorporated into the ongoing communications plan. Interactions and collaboration are reviewed throughout the project to ensure the right information is being delivered to the right people at the right time.

After the completion of the implementation project, the State will have a Contractor Contract Administrator with ongoing responsibility for the overall operational relationship overall and ultimately accountable for service delivery, relationship management and client satisfaction.

22. PROJECT CONTROL & REPORTS

Once the Project Kick-Off meeting has occurred, the Contractor Project Manager will monitor project implementation progress and report on a weekly basis to the State's Project Manager the following:

- Progress to complete milestones, comparing forecasted completion dates to planned and actual completion dates
- Accomplishments during the reporting period, what was worked on and what was completed during the current reporting period
- Indicate the number of hours expended during the past week, and the cumulative total to date for the project
- Tasks planned for the next reporting period
- Identify any existing issues which are impacting the project and the steps being taken to address those issues

- Identify any new risks and describe progress in mitigating high impact/high probability risks previously identified
- Indicate the amount of funds expended during the current reporting period, and the cumulative total to date for the project
- Provide project status reports to the SOM project team at least weekly or more frequently if requested by SOM (such as issue resolution)
- The Contractor will provide a Monthly Executive Project Control Report, and as requested by SOM, throughout the life of this project. Each report will contain the following at minimum:
 - Hours: Indicate the total hours, to date, for the project. Also state whether the remaining hours are sufficient to complete the project.
 - Accomplishments: Indicate what was worked on and what was completed during the current reporting period
 - Issues and Risks: Identify all issues, risks and change controls that have occurred on the project.
 - Funds: Indicate the amount of funds expended during the current reporting period, and the cumulative total to date for the project.

The Contractor will implement the RegSys solution for go live in 12 months from Contract execution. The project is based upon adding functions to the “out of the box” functionality of the RegSys product.

The RPM process includes extensive controls, checkpoints and reporting as these are the cornerstones for the project. The Contractor acknowledges and will fulfil the weekly reporting (Contractor Project Manager and time tracking) as well as Monthly Executive Project Control Report per this Contract.

As a registry centric methodology, the RPM process also includes additional controls and reports:

- Risk Management Plan
- Issue Management Plan
- Change Control Management Plan
- Communication Management Plan
- Quality Management Plan
- Time Management Plan

Risk Management Plan

The Contractor Project Manager is certified Project Management Institute (PMI) project management professionals (PMP) and accordingly the Contractors approach to risk management will adhere to “Project Management Body of Knowledge” (PMBOK) guidelines for this project. A risk management plan will be incorporated into the overall

project plan. A key component of this plan is a risk register. During the definition phase, a risk register will be created and maintained and managed throughout the lifecycle of the project. Risks will be identified, analyzed, planned, monitored and responded to.

The risk register will document all “known risks” and strategies will be developed to manage these risks in terms of avoiding, transferring, mitigating or accepting these risks as per the classification in terms of probability and resultant impact. The risk register will contain the following information:

Item	Description
Status	This is the status of the risk e.g., active, dormant, or rejected.
Risk Category	Each risk is categorized into one of the following categories: <ul style="list-style-type: none"> ▪ Internal ▪ External ▪ Project management risks
Risk Event	This is the actual event that the risk is attributed to.
Cause	What event could cause the risk to be realized?
Effect	What is the likely effect of this risk occurring?
Threat or Opportunity	The risk is identified as either a threat or opportunity to the project.
Primary Objective	This specifies which area of the project would be affected <ul style="list-style-type: none"> ▪ Cost ▪ Time ▪ Scope ▪ Quality
Probability	<ul style="list-style-type: none"> ▪ Low ▪ Moderate ▪ High
Impact	<ul style="list-style-type: none"> ▪ Low ▪ Moderate ▪ High
Risk Matrix	This matrix correlates the probability and the impact of this risk occurring.
Response Strategy	<ul style="list-style-type: none"> ▪ Mitigate ▪ Transfer ▪ Avoid ▪ Accept
Response Actions	The response actions that are to be undertaken should the risk occur.
Responsible Entity	The person or organization responsible for managing this risk.

Interval	The frequency that this risk is to be re-evaluated e.g., daily, weekly, monthly.
Status/Comments	Any status updates or comments related to the management of the risk.

The Contractor Project Manager will utilize experiences on other implementations to quickly identify risks to minimize and mitigate potential negative impact on the overall project.

The process of managing risk throughout the project is again governed by the principles of PMBOK. The process involves accurately documenting each risk, analyzing, and assessing the probability and impact of each risk and developing appropriate responses. The response to a risk is then assigned, actioned, and accordingly incorporated into the overall project plan.

Issue Management Plan

Within the risk management process, the Contractor will seek to identify and mitigate problems and issues before they occur. However, during any project unforeseen problems may arise, which the Contractor will manage using the Identify, Assess, Plan, and Implement approach.

The following is a standard reporting log that will be used to capture details of the problem and assign ownership:

Item	Description
Issue number	A unique number that identifies the issue that has occurred.
Status	Issues will be either opened or closed.
Priority	Each issue will have one of the following priorities: <ul style="list-style-type: none"> ▪ High; ▪ Medium; and ▪ Low.
Issue	This is a full description of the issue that has occurred.
Date reported	The date the issue was reported to the ISC project management team.
Reported by	The individual who reported the issue to the ISC project management team.
Assigned to	Each issue is assigned to a member of the ISC project management team to ensure that the issue is appropriately handled.

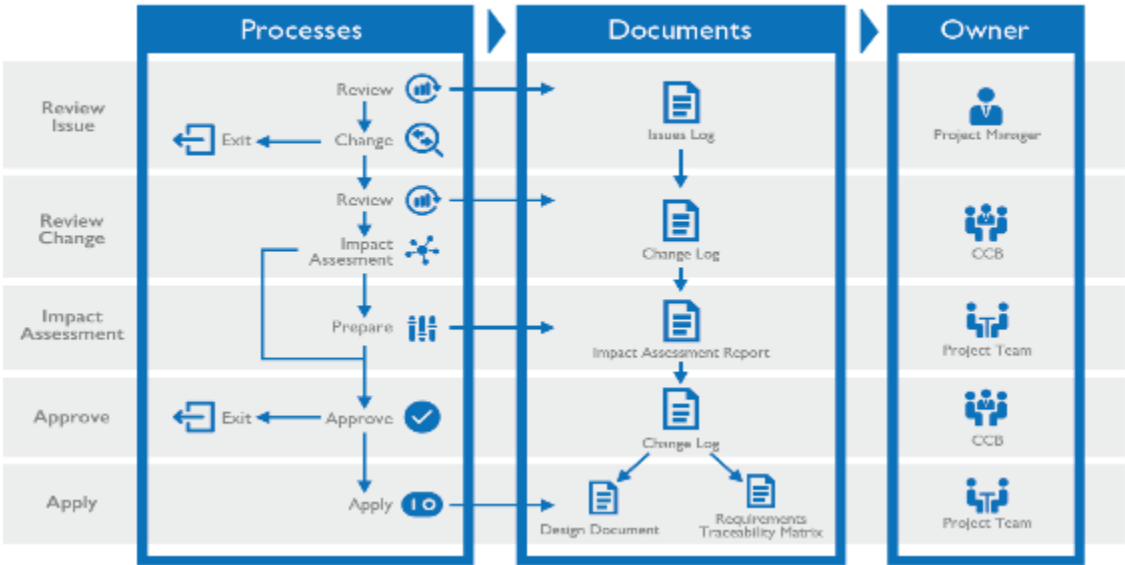
Target resolution date	The Contractor will seek to resolve each issue as quickly as possible. A target resolution date will be set once it has been assessed. The Contractor will then actively manage the issue until it is resolved.
-------------------------------	---

Where issues cannot be resolved using the agreed plan of action, the issue will be escalated to ensure a speedy resolution. The Contractor will use best practice in the escalation process to ensure the right people, at the right level and at the right time, are involved to ensure issues do not impact the project delivery. This escalation process will be agreed with the State at the start of the project.

Change Control Management Plan

The Contractor will use an iterative approach to project delivery. One of the key benefits of this approach is to allow change and user feedback to be incorporated within the implementation phase. The change control process is managed by a Change Control Board (CCB) – which will be created at the beginning of the project by the State and the Contractor. The CCB will consist of project representatives including the sponsor and the Contractor Project Managers, State Program Managers and State Project Manager.

Implementation Change Control



During the design/development sprint release session, the Contractor implementation team will record all applicable feedback to the backlog. The Contractor Project Manager and State Program Managers will assess this feedback and determine whether a

change request is required. Some of the feedback will not require a change request as these will be known issues and already scheduled for development.

Once the change request has been raised it will be assessed and, if required, the implementation team will produce a full impact and assessment report. This report will contain information on the effort and impact of the change and will be presented to the CCB. The board would assess the following guidelines for approving or rejecting change requests:

- Is the change within scope of the Contract?
- Is it feasible to incorporate the change at this stage of project?
- Can the change be born by fast-tracking project activities?
- Is the effort greater than the agreed threshold [x] of post design change days?

If no is answered on any of the questions listed above, the Contractor implementation team can present a quote for implementing the change if requested to do so by the State.

Communications Management Plan

The handling of meetings is described in Section 21, Meetings of the SOW.

Quality Management Plan

The quality management process is tightly coupled with the requirements management process, is to ensure that all elements are delivered, tested and traceable. The criteria for measuring quality for functional requirements testing will be based on the successful implementation of the required functionality. For non-functional requirements, the criteria for measuring quality will be based on the agreed measures for those requirements.

The roles and responsibilities for Quality Assurance (QA) and Quality Control (QC) are as follows:

1. The Contractor is responsible for delivering a solution that meets the agreed requirements of the State.
2. The Contractor is responsible for unit testing and system testing.
3. The State is responsible for validating integration testing, user acceptance testing, and end-to-end testing.

Time Management Plan

The Contractor will follow a common time management process for developing a schedule on adaptive projects. The following steps occur at varying levels of granularity, depending on whether the schedule is for the overall project, or an individual sprint/stage.

1. Sequencing the work based required deliverables and requirements.
2. Determining the duration required for delivery of the components.
3. Monitor the schedule, seeking timeline streamlining opportunities, the resulting schedule and look for efficiency opportunities.
4. Monitor the schedule, ensuring the project stays on-track.

The responsibility for managing the schedule belongs to the Contractor Project Manager. The business agrees to the schedule defined.

The Contractor will use standard GANTT technique/approach for tracking and communicating a project's timeline. The Contractor will utilize Azure DevOps and Microsoft Project for management and reporting.

PERT or GANTT chart display will be used to show project, task, and time relationship.

23. PROJECT MANAGEMENT

The Contractor Project Manager will be responsible for maintaining a project schedule (or approved alternative) identifying tasks, durations, forecasted dates and resources – both Contractor and State – required to meet the timeframes as agreed to by both parties.

Changes to scope, schedule or cost must be addressed through a formal change request process with the State and the Contractor to ensure understanding, agreement and approval of authorized parties to the change and clearly identify the impact to the overall project.

The Contractor must include the participation of the State of Michigan's core team which will consist of Project Manager, Product Owner, Subject Matter Experts, Testers, Analysts, and Technical Developers. The SOM core team will be appropriately allocated to participate on the project team.

The Contractor must include a comprehensive discovery phase for requirements validation, analysis, design, and product backlog development. The Contractor will lead facilitated analysis sessions and document its findings in sufficient detail to demonstrate a complete understanding of the business processes and explain how the proposed solution will meet the State's requirements. A design and development roadmap will be created by the Contractor and reviewed and approved by the State.

SUITE Documentation

In managing its obligation to meet the above milestones and deliverables, the Contractor is required to utilize the applicable State Unified Information Technology Environment (SUITE) methodologies, or an equivalent methodology proposed by the Contractor.

The Contractor will follow <https://www.michigan.gov/suite> and meet how each PMM.SEM requirement will be met.

The Contractor will submit the final plans within 14 days of notice of proceeding.

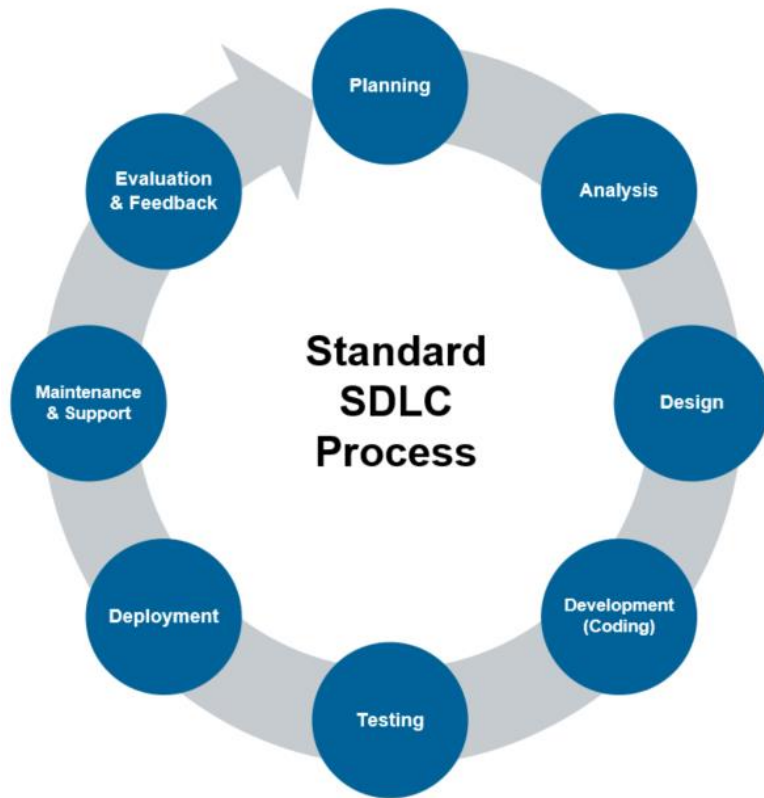
The Contractor has reviewed and will fully meet Michigan’s approach for Project Management, including the Project Management Methodology (PMM) and Systems Engineering Methodology (SEM) requirements. The Contractor Project Manager is certified Project Management Institute (PMI) project management professionals (PMP) and accordingly the Contractors approach to project management adheres to “Project Management Body of Knowledge” (PMBOK) guidelines.

The Contractor will use standard practices from the Project Management Institute, alongside Agile principles and techniques that will be used for this implementation. Contractor will use a hybrid delivery approach using Agile, and the standard PMI process groups (i.e., Initiate, Plan, Execute & Close – with the Control process group intertwined with those 4-process groups), the Contractor will use “Azure DevOps” for solution implementation control.

Each project phase will be managed by a certified Contractor Project Manager (“**PM**”) who will manage all project management activities in accordance with the Project Management disciplines. This includes but is not limited to; project scheduling, contractual stakeholder management and communication, and other project activities governed and delivered as per plan. The Contractor will also include one Product Owner (“**PO**”) who will be charged with managing the backlog and related solution requirements. The PO is the Contractor’s product representative to the State’s implementation team. The team will also consist of a system architect, quality assurance resources and technical & development resources.

SDLC for a hybrid Agile delivery

The Contractor will leverage a standard SDLC (Software Development Lifecycle) process for iterative phases within the solution delivery.



SDLC: Planning, Analysis, and Design

The Contractor will have a team consisting of a Contractor project manager, Product Owner, Contractor business analysts, Contractor technology (architect, developers, user interface/user experience (“UI/UX”) designer and quality assurance) as well as Contractor operations (registry policy, processing and customer support) personnel work with Michigan stakeholders, business and technical experts to look for refinements required to address the requirements. During the Planning, Analysis, and Design, the Contractor project manager will develop a sprint plan to deliver the outcomes for the sprint. A key output for each sprint is a project backlog, containing all known tasks to be completed during the Development, Testing, Deployment stages of the SDLC for that phase. Depending on the nature of the deployment, the completed tasks may also progress into the Maintenance & Support stage. After each phase, the project team engages in an Evaluation & Feedback stage to gain insights for the next planning & execution cycle for the project.

During Planning, Analysis, and Design, workshops will be held with the State (in-person when possible, or virtual). The workshops will further clarify requirements and user stories which will be captured in the project backlog.

SDLC: Development, Testing, and Deployment

These stages create and deliver the project backlog. The backlog will be refined to a more granular level. These stages of the SDLC uses a feedback-loop to elicit and incorporate feedback, reducing rework or wasted effort.

The Contractor will utilize Azure DevOps which works effectively with a hybrid agile project delivery,

- improving the quality of the development
- creating a faster time to go-live, and
- continually improving the Contractor processes resulting in fewer issues post-release.

The Contractor will follow standard deployment procedures before code is promoted into test or production environments. The types of tests the Contractor will use includes:

- test cases,
- automated testing,
- regression testing,
- nightly test runs,
- cyber security testing,
- user acceptance testing,
- accessibility/standards compliance testing, and
- performance testing.

The Contractor will make test cases available to business users and stakeholders through Azure DevOps. The final acceptance test by the State will determine when the functionality is ready to be deployed into a live production environment.

For data migration, the Contractor's will begin the planning through deployment of data from the legacy system as early as possible as a separate, yet related delivery stream. Starting early will allow the Contractor and the State to have early identification of data quality and data integrity issues. As early as possible, migrated data will be available in the user acceptance testing environment, pending data quality and integrity.

During Deployment into a live production environment, the Contractor and the State will have collaboratively prepared Registry personnel to deliver registry services in the new solution (e.g., through training).

SDLC: Maintenance & Support, and Evaluation & Feedback

During Maintenance & Support, the Contractor will transition the production solution to the Contractor Operations Manager for ongoing Maintenance & Support. Meetings with

the State and the Contractor will formalize the transition relationships and solidify the agreed upon approach for maintenance & support of the system.

Going forward the Contractor Service Delivery Manager will be responsible for working with the State on the ongoing support and services of the UCC solution. Development support and maintenance of the system will be provided by the Contractor support engineers in Regina, Saskatchewan, Canada. During Evaluation & Feedback, the Contractor and the State will work together to understand areas for improvement on subsequent project phases, and for ongoing operations. This will be a collaborative effort where we work together to understand, “what worked well?” and “what could have been better?”

Reporting Available After Implementation

Reporting continues to be essential after the successful implementation of the new UCC system.

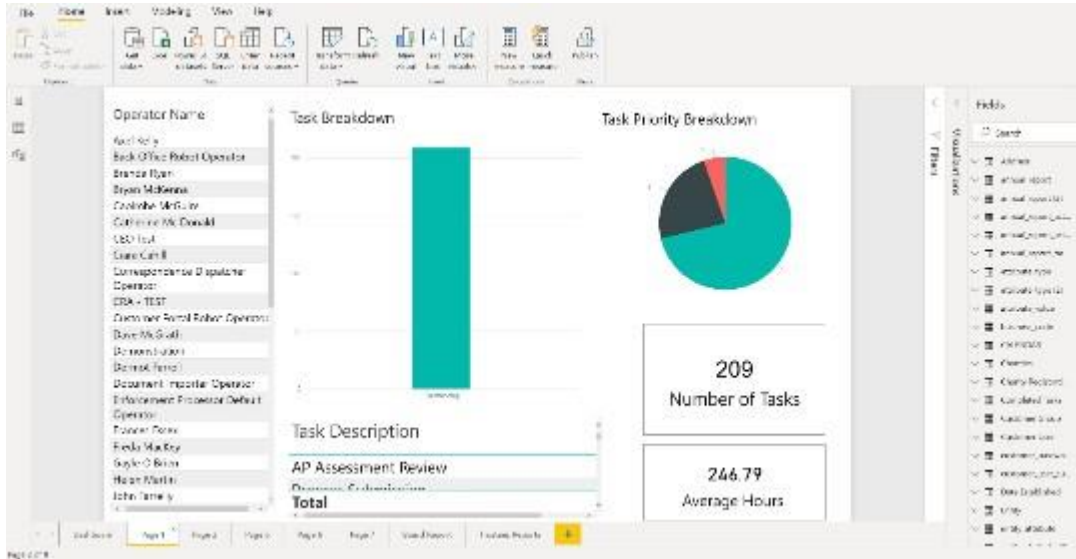
RegSys utilizes SQL Server Reporting Services (“SSRS”) to enable a suite of canned reports which are available out of the box.

Custom Reports

Pre-built reports in RegSys are developed using SSRS.

Custom reports will be developed as requested by the State. Once the output has been defined, SQL is used to generate the report query, the parameters are configured, and the output is styled to meet the standardized template. Reports can be added by the system administrator to the back-office reports menu.

The solution also provides for using Microsoft Power BI.



RegSys will have a standard set of data models which can be used by Power BI users.

Project Milestones Timeline

Milestones/Deliverables for Implementation

The Contractor's tentative hybrid agile project milestone timeline is included in Schedule B.

Contractor must provide a schedule created in collaboration with the State and approved by the State, that contains the above Associated Milestone Deliverables.

Go Live and Warranty

The Contractor must implement the solution in accordance with the agreed upon project management process, plan, timeline and methodology. The Contractor will facilitate go/no-go meetings at appropriate stage exits, determined in collaboration with the State. The Contractor will obtain written approval from the State prior to any changes or releases to the Production environment. The Contractor will inform the State prior to any changes or releases to the UAT environment. State resources that are permitted to approve changes must be identified in the Project Management Plan. The Contractor must implement the solution during non-business hours without additional costs to the State and unless otherwise approved by the State.

The Contractor will provide in-person support at a time and location determined in collaboration with the State for the purpose of GoLive support. A 90-day warranty period will follow the go live event.

The Contractor will undertake the implementation for the State from its office in Regina, Saskatchewan, Canada using only resources based in Canada. The implementation model helps to contribute to less costly implementation for the State.

State data will not leave the United States and all the State’s policies, standards and procedures will be followed.

Below are some examples of key artefacts that the Contractor will use on the project:

Examples of Project Management Document Artifacts	
Statement of Work (SOW)	Document that defines the high-level scope: <ul style="list-style-type: none"> ▪ Normally precedes initiation. ▪ Outlines the scope of work; and ▪ Outlines how and where the work will be performed.
Stakeholder Register	Document that lists and classifies all stakeholders of the project containing: <ul style="list-style-type: none"> ▪ Stakeholder name, contact details, classification, communication level, role; and ▪ Designation, designated signatory, status.
Project WBS	The Work Breakdown Structure for the project will be created and agreed.
Communication Plan	A communication plan will be established to formalize the methods and frequencies of communication between the Contractor and SOM
Data Migration Plan	A detailed plan will be created to manage the migration of data from the existing UCC system to the new data model.
Work Schedule	<ul style="list-style-type: none"> ▪ Document detailing the breakdown of requirements in to work packages. ▪ Decomposed to manageable level; and ▪ Used to create project schedule
Requirements Traceability Matrix	This document will contain a full list of the requirements with codes that relate to the items in the work schedule (and user stories and test scenarios in DevOps.
Project Schedule	The project schedule will be a living document throughout the project and will establish the timelines for implementation of the all the components in scope for the project. All components in scope will be grouped into pre- defined sprints but are subject to change. The estimates for each item will be completed during sprint planning.

Risk Register	Document listing the known project risks and response strategies.
Test Plan	The test plan will document how the Contractor will work with SOM & how the system will be tested.
Closure Report	Final delivery document including: <ul style="list-style-type: none"> ▪ Project summary. ▪ Lessons learned; and ▪ Organizational process assets.
Product Documentation & Manuals	Training, system and operational manuals including: <ul style="list-style-type: none"> ▪ Full online and back-office training manuals; and ▪ System, operational and deployment manuals.

24. TESTING

Quality Assurance

The Contractor must conduct and complete QA testing, including regression testing, prior to the State testing. Defects found during the Contractor’s QA testing must be documented in a defect tracking tool. Defects found during QA testing must be corrected before the State tests.

User Acceptance Testing (UAT)

The Contractor will provide the development of a UAT environment. UAT Testing will be conducted by the State and its selected customers. The UAT environment must (note: this is not an exhaustive list):

- accept XML filings, from both the State and its selected customers.
- create bulk data/image files in the accepted format and allow the purchase of these items. The State may require these test files be made available to selected customers for testing within their own systems.
- Connect to CEPAS and CARS to allow payment test cases to be conducted.
- Contain a link to FileNet.
- Accept State Tax Filings via the accepted electronic filing method.
- Allow for the data/image purge process to be run
- Allow testing of filing status changes

The Contractor must assist the State with developing a test plan document and test scenarios. Defects found during UAT must be addressed and corrected within a specified timeframe approved by the State in writing. The Contractor must provide

training on the application and functions within the application prior to UAT. The Contractor must be available to answer questions or address concerns during UAT.

The Contractor must provide a tracking tool for reporting defects discovered during UAT that allows the State to enter, monitor and update defect tickets. The Contractor must track defects in a clear and organized manner and provide weekly updates to the State on defect remediation.

The Contractor Quality Assurance (“QA”) team will first undertake a period of functional acceptance testing (“FAT”) on the stabilized implementation.

This will ensure that the version that is presented for User Acceptance Testing (“UAT”) will be ready for the State staff tests. The UAT period will focus on ensuring that the users of the system are able to properly use the system and ensuring that all tests are run and passed.

The quality assurance plan will be defined during the definition phase. The primary objective of testing is to assure that the system is stable and reliable while meeting the requirements. A secondary objective of testing will be to identify and expose all issues and associated risks, communicate all known issues to the project team, and ensure that all issues are addressed in an appropriate manner. As an objective, this requires careful and methodical testing of the product to first ensure all areas of the system are thoroughly examined and, consequently, all defects (bugs) found are logged and dealt with appropriately.

The Contractors overall testing process includes the following:

- **Functional Testing:** used to verify that a piece of software is providing the same output as required by the end-user or business
 - System Testing: testing of software conducted on a complete, integrated system to evaluate the system’s compliance with its specified requirements
 - Regression Testing: to confirm that a recent program or code change has not adversely affected existing features
- **Database Testing:** deals with the internal structure of the database and it is necessary to ensure that the values that an application is retrieving or storing into the database are accurate
 - Validates database tables, data models, and database schema
 - Selects default table values to check on database consistency
 - Performs module testing of database functions, triggers, views, and SQL queries
- **Non-Functional Testing:** Usability testing to determine the extent to which the software product is understood, easy to learn, easy to operate and attractive to the users under specified conditions

- **Performance Testing:** A series of load tests will be performed to ensure the system meets required performance times

The Contractor will utilize automated testing throughout the project. Test cases are written first, some may initially fail, and then software functionality is built around the tests until they pass. These automated tests allow the QA team to rapidly repeat testing on individual functions to ensure they are working fully.

Internal testing will be considered complete when the following conditions have been met:

- When QAs runs all the existing Test Cases.
- When QAs and Developers agree that testing is complete, and the system is stable.
- Testing execution of test cases has passed.
- All priority 1 (critical) bugs have been resolved and closed.
- Ad hoc testing in all areas has been complete.

In preparation for beginning the registry services, a series of load tests will be conducted to ensure the system meets required performance metrics. The Contractor will use industry standard, automated tools, such as JMeter and K6, to perform these tests. The Contractor will work with the State to determine the performance metrics. The metrics will also factor in expected traffic from potential ancillary services. Once these metrics have been established, the implementation team will create automated load and stress test scripts. The tools the Contractor will utilize allow for high-volume usage to be simulated and ramped up and down to test load, and to stress the capacity of the system.

- Azure DevOps – Test Plans
 - The Contractor will utilize Azure Test Plans to create the Contractor specific test plans, test suites, and test cases to manage and track testing for the Contractor sprints.
 - Test plans group the Contractor test suites and test cases together. This includes static test suites, requirements-based test suites, and query-based suites.
 - Test suites group test cases into separate testing scenarios. This will allow the Contractor and the State to see which fully tested scenarios are complete.
 - Test cases validate individual parts of RegSys. Test cases ensure the individual functions of RegSys have been implemented correctly and meets State requirements.
- NUnit

- The Contractor will use NUnit to perform developer configuration testing prior to implementing a feature into the test environment. Using NUnit shortens the Contractor testing life cycle by catching errors at the point of failure instead of further down the project timeline which can be costly and time intensive.
- Selenium
 - The Contractor will use Selenium to automate the test cases through the browser. Selenium will accelerate the implementation and the quality of the tests.
- Cypress
 - Additional testing protocols are complemented by Cypress, which allows us to further automate test cases. Cypress integrates with the Contractor development framework to automatically notify the Contractor developers, through the Contractor development Microsoft Teams communication channel, when a test case fails. Developers immediately resolve these bugs to ensure testing can continue to proceed on time.
- Postman
 - The Contractor will use postman during development and testing as an API testing harness. Postman provides point in time testing ability without requiring the full application in a completed state. This accelerates the Contractor implementation timelines as the Contractor will develop and test in parallel.
- SoapUI
 - The Contractor will use SoapUI to automate the Contractor API testing. The Contractor will use this in the Contractor regression tests to ensure that downstream development has not impacted upstream features that are complete. This additional rigor is just one of many elements of the Contractor quality management processes that result in dependable implementations.
- JMeter
 - The Contractor will use JMeter to load test the functional behavior of RegSys. The Contractor will also use JMeter to measure performance of RegSys ensuring that the system is ready to handle public use of RegSys.

Once the test plan has been created and approved, the QA team will create a test plan in the Test Management Tool (“TMT”). This will include tests for all in-scope requirements and tests required for accessibility and standards compliance.

Test cases will be developed on each service to enable users to conduct a thorough test on each functional requirement.

The test plan will detail all non-functional testing which will be conducted prior to transitioning the system to a production environment. The non-functional testing typically includes security and penetration testing on the host environment. Other non-functional testing activities typically adopted are on load and performance and accessibility.

When it becomes time for the User Acceptance Testing the Contractor will take the lead in providing the UAT environment. User acceptance testing is the final testing performed. This validation of the software against business requirements is carried out by the State and users who are familiar with the business requirements.

A formal "Test Plan" will be created which will define the UAT process, including agreed exit criteria. The exit criteria will determine when the project is agreed to be ready to be transitioned to a live production environment.

The Contractor QA Manager and Contractor Project Manager will work with the State to create and agree the UAT plan that is included as part of the overall test plan. The UAT plan will cover several areas of the testing process:

1. UAT Test Schedule

The Contractor QA team will collate the test cases to create an overall UAT test schedule. This will define the tests that are required to be performed, and passed, for the system to be accepted by the user. This test schedule will be broken down into the functional areas and sections within the project (E.g., corporations, UCC, financial management etc.).

2. UAT Test Efforts

The test plan will define the number and type of State staff that will be required to perform the UAT process. A responsibility chart will be created which shows which staff members are responsible for specific test cases.

The scope of the UAT environment will cover the business requirements for the fully functional UCC system, including the specific activities per Section 24, Testing within this Contract.

3. Walk Through User Reviews

The purpose of these reviews is to train the UAT testers on how to use the system and ensure they can perform the tests.

The objective of the program will be to provide user training across the RegSys application suite, relevant to specific user groups and business areas.

Training for Admins will be carried out before the before Go Live.

4. Communication Plan

Communications is key throughout the UAT process. Members of the Contractor QA team in Canada and the UAT team will stay in regular contact, holding daily calls to report on progress and to address any issues early in the testing.

5. UAT Sign-Off Process

The process for signing off the UAT will be agreed between both parties and included in the UAT plan. This will be executed once the testing has been concluded.

The UAT process is an iterative process. Once the UAT phase begins, the results of each test will be recorded, and any faults found will be documented and recorded in accordance with the testing governance plan. The Contractor QA team will analyze the test results and where required, pass the fault to the development team to fix it. This loop continues until the State is satisfied that the system is ready for go-live.

User acceptance testing is the final testing performed. This validation of the software against business requirements is carried out by the State and users who are familiar with the business requirements.

25. ADDITIONAL INFORMATION

The State reserves the right to purchase any additional services or products from the Contractor during the duration of the Contract.

SCHEDULE A – TABLE 1 – BUSINESS SPECIFICATION WORKSHEET

Instructions for Completing the Business Specifications Worksheet

Contractors must meet each business Specification.


The Business Specifications Worksheet contains columns and is defined as follows:

Column A: Business Specification number.

NOTE:

- The “**Required**” section of the Business Specifications Worksheet lists items that the State requires to be part of the Solution. “Required” items will be evaluated and scored upon per the State evaluation process.
- The “**Optional**” section of the Business Specifications Worksheet lists items that are not required at the time of the solicitation but may be desired by the State in the future. Such “Optional” items will be evaluated and used in a best value award recommendation

Column B: Business Specification description.

A	B	
Business Specification Number	Business Specification	NIST Family
	REQUIRED REQUIREMENTS SECTION 2: Security	
1.	The solution must allow for the creation of multiple user roles with varied (configurable) system access and capabilities.	
2.	The solution must allow for the disabling of any single system administrator role that would have access to both system and security related capabilities.	
3.	The solution must not store credit card information.	PCI
4.	System Roles must support separation of duties and least privilege in the production environment: A. MDOS Security Administrator <ul style="list-style-type: none"> • Able to add/disable users • Able to change user roles • Cannot do anything else in the application (ex: cannot process filings) • Security reports B. MDOS System Administrator <ul style="list-style-type: none"> • Able to edit templates & some settings • Able to edit user role functions • Cannot do anything else in the application (ex: cannot process filings) • Security Reports C. No “All Powerful” system admin user role within the application	AC
5.	System Roles – Test <ul style="list-style-type: none"> • The solution must allow for configurable roles in a test environment and allow a user switch among roles in the test environment. 	
6.	Contractor must follow the SUITE process and assist with the system security plan (SSP) process managed with the State’s Governance Risk and Compliance Tool (Keylight) (SA-02).	
7.	Contractor to provide ongoing annual contiguous SOC 2 Type II report for the Application and ongoing annual contiguous SOC 2 Type II report for Hosting (required for Contractor-hosted systems) for the five AICPA Trust	To be provided on the timeline in

A	B	
Business Specification Number	Business Specification	NIST Family
	Criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy.	Schedule E.
8.	Provide AICPA Complementary User Entity controls in place by Contractor for any subservice organizations used (AWS, Azure, etc.) as defined in the SOC report.	
9.	All SOM data must remain in the contractually agreed-upon hosting environment.	
10.	Contractor must provide a list of all subservice organizations and their associated products that are used to host, maintain, provide additional services, or build the application.	
11.	If not hosted by the State, the data (including test, production, backup/recovery data) must be hosted only in the United States.	
12.	The information system automatically inactivates State of Michigan and public user accounts after 60 days due to non-use of the system, configurable by the State of Michigan.	AC-02(3)
13.	The solution must send a notification to a role specified by MDOS, indicating a review of external (public) user access is needed.	
14.	The solution must flag inactive public users.	
15.	The solution must automatically notify the public user by email that their account is at risk of being inactivated.	
16.	The solution must allow the State of Michigan to inactivate or reactivate an inactive public user account, restricted by role-based security.	
17.	The solution must separate State of Michigan user inactivation/reactivation security privilege from public user account inactivation/reactivation privileges. As explained above, State of Michigan user access must be handled by the Security Administrator user role.	

A	B	
Business Specification Number	Business Specification	NIST Family
18.	The solution must allow public administrator/manager to deactivate and reactivate users in their group	
19.	No temporary, emergency, or group accounts i.e., only one user account per email address.	AC
20.	If not hosted by the State, the data must be hosted in a FedRAMP moderate authorized environment.	
21.	If not hosted by the State, the data must be stored in the government cloud (as opposed to commercial cloud) if one exists.	
22.	<p>The information system automatically documents account creation, modification, disabling, and removal actions and generate the below information in a report:</p> <ul style="list-style-type: none"> ▪ Each State of Michigan user account created ▪ Each security role created ▪ The privileges assigned to each security role. ▪ The security report must include user account creation, modification, inactivation, and reactivation dates. ▪ The security report must track the date a role privilege is changed. The security report must track the date of each State of Michigan user member's last system log in. ▪ The security report must be exportable to Word, Excel, or PDF. 	AC-02(4)
23.	Access to the security report must be configurable by security role.	
24.	System must not allow deletion/removal of user accounts.	
25.	The information system must terminate a user's session after a defined amount of time of inactivity, configurable by the State of Michigan.	AC-12

A	B	
Business Specification Number	Business Specification	NIST Family
26.	The information system displays a customizable and configurable message, display a warning to the of being automatically logged out of the system. Verbiage must be configurable by the State of Michigan.	
27.	The information system initiates a session lock after a defined amount of time of inactivity, configurable by the State of Michigan. The information system session lock, when activated, places a publicly viewable pattern onto the associated display, concealing what was previously visible on the screen.	AC-11 & AC-11(1)
28.	<p>The information system must be able to generate an audit report daily of the following events for State of Michigan users:</p> <ul style="list-style-type: none"> • User account management activities: Creation, Modification, or disable of accounts. • Use of Administrator privileges. • User role creation or modification • Privileges assigned to each role • User account status • Date of Last Login • List of users and their associated role • Must be exportable as PDF, MS Word, MS Excel 	AU-02
29.	<p>The information system generates audit records containing:</p> <ul style="list-style-type: none"> • Type of event that occurred. • When the event occurred. • Where the event occurred. • The frequency or count if the record represents multiple occurrences of the event. • The source of the event. • The destination of the event. • The outcome of the event. 	AU-03

A	B	
Business Specification Number	Business Specification	NIST Family
	<ul style="list-style-type: none"> • Where IP address is stored/located/identified. • Must be exportable as PDF, MS Word, MS Excel. • Must be generated on demand within a selected date range. 	
30.	<p>The solution must provide an audit trail that indicates which State of Michigan users and when the below items occurred, but not exclusive to:</p> <ul style="list-style-type: none"> - Reviewed - Approved for processing - Redacted - Edited - Updated - Voided - Deleted - Regenerated the image for - Filing revisions, including previous and revised information for comparison - Must be exportable as PDF, MS Word, MS Excel - Must be generated on demand within a selected date range. - Must allow generation based on selection of a single State of Michigan user. This criteria is an optional addition to selected date range. If no individual user is selected, report must show all State of Michigan users. 	
31.	<p>The following events will be logged, these events must be available for review through audit log report(s):</p> <ul style="list-style-type: none"> - Successful and unsuccessful system log-on attempts. 	AU

A	B	
Business Specification Number	Business Specification	NIST Family
	<ul style="list-style-type: none"> - Successful and unsuccessful attempts to use: <ul style="list-style-type: none"> o access permission on a user account, file, directory or other system resource; o create permission on a user account, file, directory or other system resource; o write permission on a user account, file, directory or other system resource; o delete permission on a user account, file, directory or other system resource; o change permission on a user account, file, directory or other system resource. - Successful and unsuccessful attempts to change account passwords. - Successful and unsuccessful actions by privileged accounts (e.g., root, Oracle, DBA, admin) - Successful and unsuccessful attempts for users to: <ul style="list-style-type: none"> o access the audit log file; o modify the audit log file; o destroy the audit log file - Must be exportable as PDF, MS Word, MS Excel - Must be generated on demand within a selected date range 	
32.	<p>The system must provide record generation capability for the following types of events:</p> <p>Database-Layer</p> <ul style="list-style-type: none"> -User account management activities -Database shutdown -Database restart -Database errors -Failed and successful log-ons 	

A	B	
Business Specification Number	Business Specification	NIST Family
	<ul style="list-style-type: none"> -Security policy/configuration modifications -Use of administrator commands -Change of password -Changes to database records Application-Layer <ul style="list-style-type: none"> -User account management activities -Application shutdown -Application restart -Application errors -Failed and successful log-ons -Security policy/configuration modifications -Use of administrator commands -Change of password -Change of application critical records. Operating System-Layer (Optional if hosted by the state) <ul style="list-style-type: none"> -User account management activities -Server shutdown -Server restart -Server errors -File creation -File deletion -File modification -Failed and successful log-ons -Security policy/configuration modifications -Use of administrator commands -Change of password 	
33.	The solution must automatically generate and send the application layer audit logs as specified by MDOS on a weekly basis.	AU-04

A	B	
Business Specification Number	Business Specification	NIST Family
34.	Sufficient audit storage capacity to support ongoing operations and rollback of the system. System sends an audit storage alert when capacity is getting low.	AU
35.	Information system must use internal system clocks mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and maintains time synchronization within 20 milliseconds of reference clocks.	AU-08
36.	The solution inputs and outputs must meet SOM standards for database security (e.g., not create, use, or rely on Microsoft Access databases or similar database software)	
37.	The Contractor must provide a document which describes the functional properties of the security controls to be employed and provide design and implementation information for the security controls and application.	SA-04
38.	<p>The Contractor must provide a document that contains comprehensive system configuration information and a technical baseline.</p> <p>The Contractor will provide a comprehensive set of system documentation for all aspects of the solution. These documents include, but are not limited to:</p> <ul style="list-style-type: none"> -System Design Documents -Technical User Documents -Non-technical (End-User) Documents -Disaster Recovery Documents 	SA-05

A	B	
Business Specification Number	Business Specification	NIST Family
39.	The system must be configured to provide only essential capabilities and restrict the use of specified functions, ports, protocols, and/or services.	CM
40.	A data dictionary must be provided to MDOS and maintained throughout the system lifecycle.	CM
41.	Provide evidence and documentation of secure coding & use of security engineering principles.	SA-08
42.	Define a written bug remediation process that includes a tracking process whereby State of Michigan and Contractor users may enter the bug, enter comments discussing additional details or solution details, attachment of screen shots, what stage of remediation the bug is in, approval of the change, and verification that the change was implemented correctly. The tracking system must assign an individual tracking number to each bug entered.	SA-10
43.	A list of protections in place that prevent unauthorized and unintended information transfer via shared system resources.	SC-04
44.	List the technologies in place to prevent Distributed denial-of-service (DDoS) attacks.	SC-05
45.	List the types of managed interfaces (firewalls, routers, subnets, etc.) that protect the boundary of the application.	SC-07
46.	Encrypts all data in flight using FIPS 140-2 certified and a cypher key strength of at least 128-bit AES and TLS 1.2, HTTPS or higher. encryption protocols. The Contractor will use a minimum	SC-8 & SC-28 & SC-13
47.	Encrypts all data at rest using a symmetric cypher that is FIPS 197 certified (AES) and at least 256-bit strength.	SC
48.	Document how encryption keys are managed and protected.	SC-11 & SC-12

A	B	
Business Specification Number	Business Specification	NIST Family
49.	The information system must conform to MDOS and/or the State of Michigan’s established record retention policies and schedules. The solutions must be able to be configured by the State to retain and automatically purge records based on retention schedules as defined by the State.	SI-12
50.	MDOS must be able to receive a copy of the data, in an agreed upon format, for records retention storage on request.	SI-12
51.	Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.	SI-03
52.	Information system must detect attacks and indicators of potential attacks in accordance with Michigan Security Operations Center (MiSOC) monitoring standards and procedures.	SI-04
53.	Employs integrity verification tools to detect unauthorized changes to software, firmware, and information.	SI-07
54.	Version control software must be used.	PD-CM1
55.	Development, Testing, and Production environments must be separated.	PD-CM2
56.	Hosted Services and the application must be scanned for vulnerabilities every month. A report of the scan results and the name of the tool used will be provided to MDOS each month. Vulnerability scan report and results must meet SOM SADLC requirements.	RA-5
57.	The vulnerability scanning tool must be updated before each scan.	RA-5 (1)
58.	Michigan Cyber Security must be permitted to scan the application for vulnerabilities.	RA-5
59.	The Contractor must keep security patches up to date and provide evidence to MDOS.	RA-5

A	B	
Business Specification Number	Business Specification	NIST Family
60.	Contractor must obtain public key certificates from an approved service provider. Contractor must keep certificates up to date and valid and provide proof to MDOS.	SC-17
61.	Application must maintain a separate execution domain for each executing process.	SC-39
62.	The vulnerability remediation timeline must be in alignment with the remediation requirements defined within State of Michigan policy, standard, and procedure.	RA-05
63.	Provides release notes on maintenance activity, patching cycles and system updates to MDOS.	MA-03
64.	Nonlocal maintenance activities may only be done through a SOM VPN.	MA-04
65.	The solution must be operational and accessible to internal State of Michigan users, and external customers 24x7x365 with a 99.98% uptime except during pre-approved maintenance windows.	
66.	The information system checks the validity of information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.	SI-10
67.	Solution must provide a customizable terms of agreement for anyone filing a financing statement with UCC. Agreement to the terms is required in order to file a statement.	PT-05
68.	Solution must track the audit trail of the agreement including the name of the person, acceptance of terms, date and time of acceptance, terms at the time of acceptance, and related financing statement filed by that person.	PT-05
69.	Solution must allow MDOS to search this audit trail, filter, and export results ad-hoc.	PT-05

A	B	
Business Specification Number	Business Specification	NIST Family
	OPTIONAL REQUIREMENTS <u>SECTION 2: Security</u>	
70.	The system will email Notification to user that account is at risk of being disabled. If email bounces back notification, disable account automatically.	
	REQUIRED REQUIREMENTS <u>SECTION 3: Public User Accounts</u>	
71.	The solution must allow State of Michigan users to indicate if a public user must pay for UCC11 searches and/or filings, restricted by role-based security.	
72.	The solution must provide the ability for external organizations (public users) to have multiple individual user accounts all billed to a single UCC billing account number.	
73.	The solution must allow for a public user role hierarchy, with manager and user roles. The final names of the hierarchy roles can be determined in discussion between MDOS and the Contractor.	
74.	The solution must allow the public user manager (or highest in hierarchy) role access to all filing acknowledgements, rejections, and UCC-11 searches performed by all users lower in their hierarchy.	
75.	The solution must allow the manager (or highest in hierarchy) to sort their filing display by users lower in the hierarchy to allow for ease of billing reconciliation.	
76.	The solution must allow public users to edit their own account information including but not limited to: <ul style="list-style-type: none"> - Name - Street address - City - State - Zip 	

A	B	
Business Specification Number	Business Specification	NIST Family
	<ul style="list-style-type: none"> - Email address - Phone number 	
77.	The solution must allow the manager user (or highest in hierarchy) role to edit user account status for users lower in their hierarchy.	
	<p>REQUIRED REQUIREMENTS</p> <p><u>SECTION 4: State of Michigan User</u></p>	
78.	<p>State of Michigan User must be able to configure/edit/modify/update, restricted by role-based security:</p> <ul style="list-style-type: none"> - Secretary of State’s name, address, phone number, email and signature on documents, templates, and website pages - UCC filing office name, street address, phone number, and email address on documents, templates, and website pages - Website addresses and links - All templates and output documents - If a web-based solution, header, footer and graphic of the website - List of key words for fraudulent filings - Country codes - Country names - Instructions displayed on-screen throughout filing or search flows <ul style="list-style-type: none"> o Different than instructions provided through a ‘help’ button 	
79.	The solution must limit State of Michigan users who can create filings to be designated by security role.	
80.	The solution must allow State of Michigan users to set the filing date and time for filings processed using the State of Michigan module.	

A	B	
Business Specification Number	Business Specification	NIST Family
81.	The solution must allow the selection of different delivery methods. The delivery method will dictate the filing date and time. In this requirement delivery method means how a filing is submitted to the State of Michigan for processing.	
82.	The solution must allow State of Michigan users to review all UCC filings submitted through the public filing portal before the filing is considered processed and filed.	
83.	The solution must allow filings submitted through the public filing portal to be approved through the review process. If approved, an initial filing number, filing date and time must be assigned equal to the date and time, down to seconds, the public user selected submit.	
84.	The solution must place filing submitted through the public filing portal to be approved in a “Review Queue” in the order in which they were submitted, by the date they were submitted.	
85.	Once filings are in the queue by date, the system must put them in order by time submitted. Time submitted will be broken down to seconds. For example, a filing submitted on June 1 at 10:14:14 am will be reviewed before a filing submitted on June 1 at 10:14:15 am.	
86.	The solution must continuously update the review queue as new filings are submitted.	
87.	The solution must provide a way to view how many (the count) filings are in the queue to be reviewed.	
88.	The solution must allow access to view how many filings are in the queue to be restricted by role-based security.	
89.	The solution must continuously update the count of filings in the queue to be reviewed.	
90.	The solution must allow the UCC supervisor to see a list of all filings in the queue and allow them to view a selected filing.	

A	B	
Business Specification Number	Business Specification	NIST Family
91.	The solution must return a filing to the review queue if the State of Michigan user reviewing it logs out or has their session terminated prior to approval.	
92.	The solution must return the filing to the review queue in a position, so it is the next pulled for review. Filings returned to the queue must be reviewed before filings submitted after it. (i.e., first in first out)	
93.	The solution must allow State of Michigan user to manually return a filing to a "Review Queue".	
94.	The solution must allow an ability to manually redact information.	
95.	The solution must allow for redaction of the first five (5) digits of a social security number (SSN) if it is included in the collateral section or on an attachment.	
96.	The solution must flag filings as suspect (potential fraud) based on key words entered in the debtor's name or collateral fields. A list of key words will be provided at a later date.	
97.	The solution must allow State of Michigan users to accept (i.e., process) or reject, restricted by role-based security, suspect filings during the review process.	
98.	The solution must allow State of Michigan user to select to generate a debtor notification letter if the filing is suspect and the debtor is designated as an organization. Additional requirements indicate the system automatically creates debtor notification letters for individuals.	
99.	The solution must allow for rejection of all filing types through the review process based on reasons set forth in MCL 440.9516 and MCL 440.9520(5).	
100.	The solution must allow State of Michigan users to select one or more of the rejection reasons.	

A	B	
Business Specification Number	Business Specification	NIST Family
101.	The solution must include a free form text box for State of Michigan users to enter additional rejection details if necessary.	
102.	The solution must create a rejection letter detailing the rejection reason(s) and any additional text from the free form text box.	
103.	The solution must provide electronic delivery of rejected filings, including the rejection letter, in the same manner as filings which are accepted for processing.	
104.	The solution must store the original filing date and time of all rejected filings in case a filing is rejected in error. The original date and time must be used when the filing is made available for searching.	
105.	The solution must exclude UCC-11 search requests from the review queue. Search requests must be completed as soon as payment is received.	
106.	The solution must exclude all filings submitted via XML from the review queue.	
107.	The solution must allow State of Michigan users to change the filing type in the "Review Queue". For example, a sovereign citizen files against themselves and selects manufactured home.	
108.	The solution must prevent State of Michigan users from editing debtor, secured party, assignee, assignor, and collateral information entered by the filer, in the Review Queue.	
109.	The solution must allow State of Michigan users to search for public user accounts by one of the following parameters: UCC billing account number, user login ID, username, first name, last name, organization name, or user email address.	

A	B	
Business Specification Number	Business Specification	NIST Family
110.	The solution must allow State of Michigan users, when viewing the public users account to select and view each filing or search individually.	
111.	The solution must display UCC-11 search criteria exactly as entered by the public user to the State of Michigan User in order for the State of Michigan user to assist the public user in obtaining the correct search results.	
112.	The solution must display an individual debtor name in fields as entered including separating first name, surname, suffix etc. into individual fields, for UCC-11 searches.	
113.	The solution must display an organization debtor name as entered in the single organization debtor name field, for UCC-11 searches.	
114.	The solution must display if copies were requested on the UCC-11.	
115.	The solution must display the date range entered if a specific time period is entered on the UCC-11.	
116.	The solution must display the name of the city entered if the UCC-11 was limited to a specific city search.	
117.	<p>The solution must allow State of Michigan users to edit information associated with a public user account including but not limited to:</p> <ul style="list-style-type: none"> - Name - Street address - City - State - Zip - Email address - Phone number - Billing account number - XML registered eCheck account number 	

A	B	
Business Specification Number	Business Specification	NIST Family
	<ul style="list-style-type: none"> - Ability to indicate the user account is eligible for no fee UCC filings or State Tax Liens. (There are 20 billing accounts that are exempt from paying filing fees.) - Ability to indicate the user account is eligible for no fee UCC-11 searches - Ability to indicate the user account is eligible to submit XML filings - User account status (active/inactive) <p>The information listed above can be edited at any time.</p>	
118.	The solution must permanently store the billing account numbers or eCheck numbers.	
119.	The solution must allow the billing account number to be associated with more than one public user account.	
120.	The solution must allow State of Michigan users to void a work order before the filing is processed, restricted by role-based security. Note: this is NOT the same as deleting a filing.	
121.	The solution must require State of Michigan users to enter a reason for voiding the work order before the void can be completed.	
122.	The solution must retain information about the voided work order in an audit table, but not display these work orders in bulk data files or on reports.	
123.	The solution must retain the voided work order number, reason for void, and name of State of Michigan user member who voided the work order.	
124.	The solution must allow State of Michigan users to enter billing account numbers and payment ID numbers to indicate proper payment has been received for a filing or UCC-11 search.	

A	B	
Business Specification Number	Business Specification	NIST Family
125.	The solution must allow State of Michigan user to select a public user for the completed filing or search to be delivered to via electronic delivery.	
126.	The solution must provide multiple ways to search for the correct public user including but not limited to username, unique identifying number, or first/last name.	
127.	The solution must accept entry of multiple payment IDs. This is necessary if the filing was initially rejected for not submitting the proper fee and the filing was resubmitted with the difference.	
128.	The solution must accept UCC-7 Affidavit of Fraudulent Filing filings.	
129.	The solution must allow State of Michigan Users to file an unlimited number of UCC-7s against the same UCC record.	
130.	The solution must change the filing status to terminated when the first UCC-7 is filed.	
131.	The solution must prevent a UCC-7 from being filed if the initial filing has lapsed.	
132.	The solution must create a letter of notification to be sent to the filer when a UCC-7 is processed, to be printed to mail. Content of the notification will be provided at a later date. Content of notification letter will be configurable by State of Michigan users, restricted by role-based security.	
133.	The solution must allow State of Michigan users to process rejections and partial rejections. Note: This is separate from the ability to process rejections in the Review Queue discussed in earlier requirements.	
134.	The solution must allow the State of Michigan user to select print or electronic delivery of full and partial rejections.	

A	B	
Business Specification Number	Business Specification	NIST Family
135.	The solution must allow State of Michigan users to reject a filing for any reason set forth in MCL 440.9516 or 440.9520(5).	
136.	The solution must allow State of Michigan users to select one of the rejection reasons set forth in MCL 440.9516 or 440.9520(5).	
137.	The solution must allow State of Michigan users to reject a filing if the initial filing number was entered incorrectly.	
138.	The solution must allow rejections of all filing types.	
139.	The solution must include a free form text box for State of Michigan users to enter additional rejection details if necessary.	
140.	The solution must create a rejection letter detailing the rejection reason.	
141.	The system must create a rejection letter detailing the portion of the filing which was rejected when a partial rejection is processed.	
142.	The system must assign an initial financing statement number, filing date and filing time for the portion of the filing which was accepted when a partial rejection is processed. A copy of the accepted filing must be electronically delivered.	
143.	The solution must allow State of Michigan user to edit filing records at any time during the life of the record.	
144.	<p>The solution must allow State of Michigan user to edit/configure the following:</p> <ul style="list-style-type: none"> - filing type - lapse date - debtor name - debtor address - filing date - filing time 	

A	B	
Business Specification Number	Business Specification	NIST Family
145.	The solution must save all revisions to the UCC database.	
146.	The solution must include any revisions in the earliest bulk data and image files generated after the revisions are saved to the UCC database. The bulk files must include an indicator to show the record is a revision of the original record.	
147.	The solution must use the revised debtor name information for UCC11 search requests subsequent to the revisions.	
148.	The solution must allow State of Michigan users to regenerate or rescan an image from a filing, attach the image to the corresponding data in the UCC database and send the image to FileNet (or similar image storage solution) to replace the incorrect/missing image.	
149.	The solution must ask if a Filing Officer Statement is required if the filing is being revised.	
150.	The solution must include a free form text box labeled "The inaccuracy or mistake on the part of the Filing Office:"	
151.	The solution must provide a free form text box labeled "Filing Office Administrative Action taken as a result of inaccuracy or mistake:"	
152.	The solution must assign a filing statement number to the Filing Officer Statement and associate it with the Initial Financing Statement record.	
153.	The solution must include the Filing Officer Statement in the earliest bulk data and image files generated after the statement is created.	
154.	The solution must include Filing Officer Statements in UCC-11 search results as part of the filing record.	
155.	The solution must allow State of Michigan user to delete filings from the database restricted by role-based security.	

A	B	
Business Specification Number	Business Specification	NIST Family
156.	The solution must allow State of Michigan user to reinstate a filing that was improperly deleted, restricted by role-based security. A reinstated filing must retain its original financing statement number and original lapse date	
157.	The solution must provide a verification queue or other method that must allow a supervisor or trainer to review a new employee's work before the filing is finalized.	
158.	The solution must allow access to review filings in the verification queue to be restricted by role-based security.	
159.	The solution must list filings in processing order in the verification queue. This must be done for ease and timeliness of review.	
160.	The solution must allow a State of Michigan users to be assigned to the verification queue based on their user role.	
161.	The solution must allow a percentage of filings, including rejections, to be assigned to the verification queue such as 25%, 50%, 75%, and 100%, configurable by user role and restricted by role-based security.	
162.	The solution must allow the percentage to be changed by State of Michigan users, restricted by role-based security	
163.	The solution must prevent the filings assigned to the queue to be finalized and delivered electronically until reviewed and approved by the supervisor or trainer.	
164.	The solution must prevent rejected filings assigned to the queue to be finalized and be delivered electronically until the supervisor or trainer approves them.	
165.	The solution must display the scanned image for review as part of the verification of indexing. This must allow the supervisor or trainer to see the image quality to	

A	B	
Business Specification Number	Business Specification	NIST Family
	determine if there is a need to rescan or clean the State of Michigan user's scanner.	
166.	The solution must allow the supervisor or trainer to assign a filing from the verification queue back for correction to the State of Michigan user who originally processed it.	
167.	The solution must allow entry of comments to explain why the filing is being sent back for correction.	
168.	The solution must allow the filing to be edited when it is assigned back to the State of Michigan user.	
169.	The solution must limit the filing types being sent to the verification queue. UCC-3 Terminations and UCC-3 Continuations may be excluded from verification.	
170.	The solution must allow work orders to be deleted from the verification queue and require entry of a deletion reason by the supervisor or trainer.	
171.	The solution must store the deleted work order, name of State of Michigan user performing the deletion, and reason for deletion in an audit table in the database.	
172.	The solution must allow State of Michigan users to scan paper filing documents as part of the filing process.	
173.	The solution must allow for scanning of high page counts (ex. 150 pages).	
174.	<p>The solution must merge all pages into one document regardless of the number of pages scanned and if scanned separately.</p> <p>This requirement is due to UCC's current scanners not having feeder tray capacity to scan more than 50 pages at a time.</p>	
	<p>OPTIONAL REQUIREMENTS</p> <p><u>SECTION: State of Michigan User</u></p>	

A	B	
Business Specification Number	Business Specification	NIST Family
175.	The solution should allow State of Michigan users to mark public user accounts as trusted.	
176.	The solution should exclude filings submitted by trusted public user from the review queue.	
177.	The solution should restrict the ability to mark public user accounts as “trusted” by role-based security.	
178.	The solution should allow State of Michigan users to upload filing document files as part of the filing office process. Acceptable file formats can be determined at a later date.	
179.	The solution should allow upload file size up to 10 MB.	
180.	<p>The solution should have a “Review Queue” that allows State of Michigan users view only access to public user accounts for the purpose of providing assistance with navigation of the new application to public users.</p> <ul style="list-style-type: none"> - For example, with the new system a user may call in unable to locate past filings. This functionality must allow State of Michigan users to see the same screen they are and navigate the public user to the exact location/item. 	
	<p>REQUIRED REQUIREMENTS SECTION 5: FILING REQUIREMENTS</p>	
181.	The solution must require a minimum of one debtor name and one secured party name with: street address, city, state, and zip code for all UCC-1 Initial Financing Statements.	

A	B	
Business Specification Number	Business Specification	NIST Family
182.	If the selected country is United States, the solution must require completion of the state field.	
183.	The solution must allow selection of a country other than the United States.	
184.	The solution must change the state field to province if a country other than United States is selected and must allow but not require the province field to be completed.	
185.	The solution must allow character number minimums in all fields as set forth by the International Association of Commercial Administrators (IACA). Final field lengths may be determined through discussion between MDOS and Contractor.	
186.	The solution must accept all numerals, letters and characters (not emojis) available on a standard English keyboard for all fields. This requirement is not applicable to the contents of attachments submitted through any filing channel.	
187.	The solution must require the user to select a filing type. Example: <ul style="list-style-type: none"> - UCC-1 Initial Financing Statement - UCC-3 Amendment Financing Statement UCC-5 Information Statement	
188.	The solution must accept UCC-1 Initial Financing Statements and require the user to select a filing sub-type. Example: <ul style="list-style-type: none"> - UCC-1 Initial Financing Statement <ul style="list-style-type: none"> o Initial Financing Statement o Manufactured Home o Transmitting Utility o Public Finance 	

A	B	
Business Specification Number	Business Specification	NIST Family
189.	<p>The solution must require the user to select a sub type and sub-sub-type if a UCC-3 Amendment Financing Statement is selected:</p> <ul style="list-style-type: none"> - Continuation - Termination - Assignment - Party Information Change <ul style="list-style-type: none"> o Debtor Add o Debtor Delete o Debtor Change o Secured Party Add o Secured Party Delete o Secured Party Change - Collateral Change <ul style="list-style-type: none"> o Collateral Add o Collateral Delete o Collateral Restate - Collateral Assignment 	
190.	<p>The solutions UCC-1 sub-type must determine lapse date.</p> <ul style="list-style-type: none"> - UCC-1 Initial Financing Statement <ul style="list-style-type: none"> o Initial Financing Statement <ul style="list-style-type: none"> ▪ Lapse date five (5) years from the filing date o Manufactured Home <ul style="list-style-type: none"> ▪ Lapse date 30 years from the filing date o Transmitting Utility <ul style="list-style-type: none"> ▪ Lapse date is indefinite from the date of filing o Public Finance <p>Lapse date is five (5) years from the filing date</p>	

A	B	
Business Specification Number	Business Specification	NIST Family
191.	The solution must require entry of the Initial Financing Statement number the amendment must correspond to when UCC-3 filing type is selected.	
192.	The solution must not allow any type of UCC-3 Amendment Financing Statements to be filed after the Initial Financing Statement has lapsed.	
193.	The solution must store the filing type, sub-type, and sub-sub-type (i.e., Transmitting Utility) in the system database.	
194.	The solution must allow entry of multiple debtors, secured parties, or both.	
195.	The solution must allow the selection of debtor type of organization or individual for each debtor being entered.	
196.	The solution must allow selection of secured party type of organization or individual for each secured party being entered.	
197.	The solution must allow an optional assignor checkbox to be selected.	
198.	The solution must allow, but not require, entry of collateral by the public user.	
199.	The solution must allow a maximum of 64,000 characters in the collateral field.	
200.	The solution must display an instruction statement above the collateral entry field that SSN and FEIN will not be included in collateral or collateral attachments. Contractor and State of Michigan may determine exact verbiage at a later time. Text must be editable by State of Michigan users, restricted by role-based security.	
201.	The solution must allow, but not require, for the selection of Collateral is held in trust or is being administered by a Decedent's Personal Representative. Only one may be selected, not both.	

A	B	
Business Specification Number	Business Specification	NIST Family
202.	The solution must allow, but not require, for selection of Agricultural Lien or Non-UCC filing. Only one may be selected, not both.	
203.	The solution must allow, but not require, for selection of: <ul style="list-style-type: none"> - Lessee/Lessor - Consignee/Consignor - Seller/Buyer - Bailee/Bailor - Licensee/Licenser 	
204.	The solution must allow for, but not require, completion of an Optional Filer Reference Data field up to 80 characters.	
205.	The solution must allow, but not require, free-form text entry in a miscellaneous field up to 100 characters.	
206.	The solution must allow an unlimited number of UCC-3 Termination amendments to be filed against a UCC-1 Initial Financing Statement.	
207.	The solution must not change the lapse date or status of a filing, including Transmitting Utility filings, when UCC-3 Terminations are filed.	
208.	The solution must prevent UCC-3 Terminations from being filed after the initial financing statement has lapsed and display an error message "Termination cannot be filed. Filing has lapsed."	
209.	The solution must allow UCC-3 Continuations to be filed only during the six-month period prior to the lapse date.	
210.	The solution must allow an unlimited number of UCC-3 Continuations to be filed during the six-month period prior to the lapse date.	
211.	The solution must only extend the lapse date when the first UCC-3 Continuation is filed.	
212.	The solution must prevent UCC-3 Continuations from being filed after the lapse date and display an error	

A	B	
Business Specification Number	Business Specification	NIST Family
	message "Continuation cannot be filed. Filing has lapsed."	
213.	The solution must prevent UCC-3 Continuations from being filed before the six-month window and display an error message "Continuation cannot be filed. Outside continuation period." Specific verbiage can be determined at a later time.	
214.	The solution must allow an unlimited number of UCC-3 Assignments to be added to the filing record.	
215.	The solution must prevent UCC-3 Assignments from being filed after the lapse date and display an error message "Assignment cannot be filed. Filing has lapsed."	
216.	The solution must allow, but not require, an assignor.	
217.	The solution must allow, but not require, selection of a secured party of record to be shown as the assignor.	
218.	The solution must allow, but not require, entry of an assignor's name and address. Assignor may be an individual or organization.	
219.	The solution must require entry of at least one assignee name and address.	
220.	The solution must allow the assignee to be designated as an individual or organization.	
221.	The solution must allow, but not require, entry of collateral information by public user for specified filing type, sub-types and sub-sub-types. List of types to be discussed by MDOS and Contractor.	
222.	The solution must prevent deleting secured parties of record when a UCC-3 Assignment is filed. All secured party names must be shown in the filing record and returned on a search report until the filing is no longer searchable.	

A	B	
Business Specification Number	Business Specification	NIST Family
223.	The solution must allow an unlimited number of debtors or secured parties to be: added, deleted, or changed on UCC-3 Amendments.	
224.	The solution must prevent debtor or secured party change amendments if the initial financing statement is lapsed.	
225.	If debtor or secured party delete is selected, the solution must display the delete in the filing record, but not remove any debtor or secured party information from the database or the filing record. All secured party and debtor names must be shown in the filing record and returned on a search report until the filing is no longer searchable	
226.	The solution must accept an unlimited number of UCC-5 Information Statement filings.	
227.	The solution must prevent UCC-5 Information Statement filings after the initial filing has lapsed.	
228.	The solution must require entry of the initial financing statement number to which the UCC-5 relates.	
229.	The solution must require entry of the financing statement number to which the UCC-5 relates. This may be the initial financing statement number or the filing number of an amendment.	
230.	The solution must display both financing statement numbers (as described in the two immediately preceding requirements) on the filing acknowledgement image.	
231.	The solution must display a draft of the filing prior to submission.	
232.	The solution must allow the user to navigate back to any previous screens to edit entered information including but not limited to the debtor, secured party, and collateral screens.	

A	B	
Business Specification Number	Business Specification	NIST Family
233.	The solution must allow the user to attach a document when they navigate back to the collateral screen from the draft review screen.	
234.	The solution must allow the user to delete a previously added attachment and add a different one.	
<p align="center">REQUIRED REQUIREMENTS</p> <p align="center"><u>SECTION 6: State & Federal Tax Filings</u></p>		
235.	<p>The solution must allow the creation of a secured party to be automatically added to Tax Lien filings and allow State of Michigan users to edit and add new secured parties name and address, restricted by role-based security:</p> <ul style="list-style-type: none"> - Michigan Treasury - IRS - Others as needed 	
236.	The solution must allow acceptance of State Tax Filings through XML or other electronic means. The Contractor must meet with MDOS, DTMB and State Tax Filing (Department of Treasury) to discuss the final solution.	
237.	The solution must allow all State Tax Filings to be completed at no fee regardless of filing channel.	
238.	<p>The solution must allow filing of State Tax types and sub-types.</p> <p>Example:</p> <ul style="list-style-type: none"> - Initial State Tax Lien <ul style="list-style-type: none"> o Note: Active seven years, 60 days - State Tax Lien Reinstatement - State Tax Lien Revocation of Release - State Tax Lien Party Amendment - State Tax Lien Release <ul style="list-style-type: none"> o Note: The solution must not change the filing status when a release is filed. The 	

A	B	
Business Specification Number	Business Specification	NIST Family
	filing must remain active until the seven-year lapse date is reached. <ul style="list-style-type: none"> - State Tax Lien Withdrawal - State Tax Lien Correction Note: Full list to be provided at a later date	
239.	The solution must allow filing of Federal Tax types and sub-types. Example: <ul style="list-style-type: none"> - Federal Tax Initial Financing Statements <ul style="list-style-type: none"> o Note: Active for 10 years, 30 days - Federal Estate Tax Lien Initial Financing Statement <ul style="list-style-type: none"> o Note: Active indefinitely - Federal Tax Liens <ul style="list-style-type: none"> o Federal Tax Lien Refile o Federal Tax Lien Release o Revocation of Release of Notice of Federal Tax Lien o Withdrawal of Notice of Federal Tax Lien o Certificate of Discharge of Property - Federal Estate Tax - Federal Justice Department <ul style="list-style-type: none"> o Federal Justice Department Amendment o Federal Justice Department Correction Filings <ul style="list-style-type: none"> ▪ Note: only allow State of Michigan users to scan document - Pension Benefit Guaranty Corporation Note: Full list to be provided at a later date	
240.	The solution must allow Federal Tax liens to be refiled (i.e., continued) at any time as long as the refile occurs before the lapse date.	

A	B	
Business Specification Number	Business Specification	NIST Family
241.	The solution must update the Federal Tax liens lapse date an additional 10 years, 30 days from the current lapse date when the refile is processed.	
242.	The solution must allow Amendment to be selected as the filing action for a Federal Tax Lien.	
243.	The solution must allow Amendment Party to be selected as the filing action for a Federal Tax Lien.	
244.	The solution must allow the entry of a Notice of Federal Tax Lien Initial or Refile financing statement number when Release of Federal Tax Lien is the selected filing sub-type.	
245.	The solution must allow multiple Certificates of Release of Federal Tax Lien to be processed prior to the lapse date.	
246.	The solution must not change the filing status of a Federal Tax Lien regardless of the number of Certificates of Release that have been filed.	
247.	The solution must not change the lapse date of a Federal Tax Lien regardless of the number of Certificates of Release that have been filed.	
248.	The solution must allow selection of Partial Release for Federal Tax Liens and allow multiple partial releases to be filed.	
249.	The solution must not change the filing status or lapse date of a Federal Tax Lien regardless of the number of partial releases filed.	
	<p>REQUIRED REQUIREMENTS</p> <p><u>SECTION 7: UCC-11 SEARCHES</u></p>	
250.	The solution must require users to log in to initiate a UCC-11 search and to retrieve electronically delivered UCC-11 search results.	

A	B	
Business Specification Number	Business Specification	NIST Family
251.	The solution must allow for UCC-11 record requests through the UCC external and internal sites.	
252.	The solution must complete UCC-11 record requests in a first-in, first-out manner.	
253.	The solution must adhere to the IACA Standard Search Logic.	
254.	<p>The solution must allow a search by:</p> <ul style="list-style-type: none"> - Debtor name <ul style="list-style-type: none"> o only allow one debtor name to be entered per UCC-11 o allow selection of individual or organization <ul style="list-style-type: none"> ▪ If the debtor is an organization, the solution must require entry of an organization name. ▪ If the debtor is an individual, the solution must require entry of a last name and must allow but not require entry of a first name, middle name, or suffix. - Filing number <ul style="list-style-type: none"> ▪ Allow selection of related documents ▪ No more than 5 filing numbers at once ▪ Allow removal of filing number 	
255.	The solution must prevent searching by secured party name.	
256.	<p>The solution must allow the following search options and sub options if debtor name is selected:</p> <ul style="list-style-type: none"> - One of the following options: <ul style="list-style-type: none"> o Search Certificate o Search Certificate and Copies o Face Copies 	

A	B	
Business Specification Number	Business Specification	NIST Family
	<ul style="list-style-type: none"> ▪ Note: Face copies are copies of only the first page of financing statements and tax liens - One of the following options: <ul style="list-style-type: none"> ○ All filings <ul style="list-style-type: none"> ▪ Note: includes lapsed financing statements ○ Un-lapsed Financing Statements only - Additional Options: <ul style="list-style-type: none"> ○ A specific time period by allowing user to select a date range ○ include related documents outside the time period ○ City <ul style="list-style-type: none"> ▪ Note: only one city name at a time 	
257.	The solution must include a search report if the UCC-11 Search is for a debtor name.	
258.	The search report must include the following: <ul style="list-style-type: none"> - the date the search was processed - the filing through date - Debtor name, as entered by the user when the search was requested - The search option selected by the user: <ul style="list-style-type: none"> ○ Search Certificate ○ Search Certificate and Copies ○ Face Copies - The search option selected by the user: <ul style="list-style-type: none"> ○ All filings ○ Un-lapsed Financing Statements only - Time period, if user performed a search by date range 	

A	B	
Business Specification Number	Business Specification	NIST Family
	<ul style="list-style-type: none"> - Name of city entered, if user performed a search by city - UCC-1 filings, State Tax Liens, Unemployment Tax Liens, and Federal Tax Liens in order of filing date and time <ul style="list-style-type: none"> o Initial financing statement or tax lien must be listed first for each filing record o Corresponding initial filing number o Corresponding initial filing date and time o Lapse date for each initial filing o With the corresponding UCC-1 Initial Financing Statement, in order of filing date and time <ul style="list-style-type: none"> ▪ UCC-3 Amendments ▪ UCC -5 Information Statements ▪ UCC Filing Office Statements ▪ UCC-7 Affidavit of Fraudulent Filing o State Tax Amendment filings in order of filing date and time with the corresponding State Tax Initial Filing. o State Unemployment Tax Amendment filings in order of filing date and time with the corresponding initial Unemployment Tax filing o Federal Tax Amendment Filings in order of filing date and time with the corresponding Federal Tax Initial Filing. o Secured Party and debtors names and addresses, affiliated with each filing record 	
259.	The solution must provide copies of the financing statements and any related documents requested for filing number searches.	
260.	The solution does not need to produce a search report for filing number searches.	

A	B	
Business Specification Number	Business Specification	NIST Family
261.	The solution must provide a payment receipt for the UCC-11 search. Content requirements will be provided later.	
262.	The solution must include a certification/affirmation statement. Content will be provided later.	
263.	The solution must provide an impression of the official MDOS seal when a certified search is requested and paid for. Image, configurable by State of Michigan restricted by role-based security, to be provided later.	
264.	The solution must include the option to purchase: <ul style="list-style-type: none"> - filing image copies - copies of all UCC, state tax and federal tax filings in the debtor's record ONLY UCC filings in the debtor's record	
265.	The solution must provide filing image copies in the same filing order number as shown on the search report regardless of input channel.	
266.	The solution must prevent charging for filing image copies of federal tax liens and filing officer statements.	
267.	The solution must provide electronic delivery of UCC11 search results including the search report and copies (if applicable).	
268.	The solution must make the search results and copies, if applicable, available to the public customer for a minimum of 90 days.	
269.	The solution must prevent deleted filings from being included on a UCC-11 Search report.	
270.	The solution must prevent image copies of deleted filings from being included in a UCC-11 Search with copy request.	
271.	The solution must allow State of Michigan users to select "no fee" for a UCC-11 initiated in the State of Michigan users portion of the solution. This may be due	

A	B	
Business Specification Number	Business Specification	NIST Family
	to an incorrect search being replaced by State of Michigan users.	
272.	The solution must provide a report to display any searches that fail to complete, that includes a reason in plain English describing what caused the search to fail.	
273.	The solution must provide a way for State of Michigan users to regenerate a failed search and deliver the regenerated search electronically.	
274.	The solution must provide a way for State of Michigan users to force delivery of a completed search or regenerated search if it did not get properly delivered to the customer using the solution's electronic delivery method.	
275.	The solution must offer non-standard search logic in a separate system flow from a standard search logic to prevent customer confusion over the type of search they are performing.	
	<p>REQUIRED REQUIREMENTS</p> <p><u>SECTION 8: Public Debtor Name Quick Search</u></p>	
276.	The solution must offer a Debtor Name Quick Search that does not require a user to log in to MI Login.	
277.	The solution must provide search results using IACA Standard Search Logic.	
278.	The solution must display a list of active and lapsed initial UCC-1, State Tax, State Unemployment Tax and Federal Tax filings.	
279.	The list must only include the debtor's name, financing statement number, lien type, filing date, filing status and lapse date.	
280.	The solution must only display lapsed filing that are still searchable during the one-year period following the lapse date.	

A	B	
Business Specification Number	Business Specification	NIST Family
281.	The solution must prevent access to filing images through the Debtor Name Quick Search.	
282.	The solution must allow the Debtor Name Quick Search results to be exported to a Word document, Excel spreadsheet, or PDF document.	
283.	The solution must not charge a fee for the Debtor Name Quick Search.	
284.	The solution must display the debtor’s name searched on the results screen and exported document.	
	<p>REQUIRED REQUIREMENTS</p> <p><u>SECTION 9: State of Michigan User Search</u></p>	
285.	The solution must allow State of Michigan users to search XML filings by filing date, filing type, filer name, or filing status and include the filing image in the search results.	
286.	The solution must include a way for State of Michigan users to download the XML code submitted for each filing.	
287.	The solution must provide a way for State of Michigan users to search all UCC, State tax, State Unemployment Tax and Federal tax liens.	
288.	The solution must list results according to retention schedule rules. Retention schedule rules will be provided in a later section.	
289.	<p>The solution must allow searching by one of the following:</p> <ul style="list-style-type: none"> - filing number - debtor name - secured party - Filing date range - Lapse date range - Filer username 	

A	B	
Business Specification Number	Business Specification	NIST Family
	- Other filer ID that may be system generated	
	The solution must display a list of all filings in the filing record related to the filing number entered in the search.	
290.	The solution must allow State of Michigan users to indicate if the debtor or secured party is an individual or organization.	
291.	The solution must display all financing statements, state tax liens, State Unemployment Tax liens, and federal tax liens associated with a debtor name based on UCC-11 standard search logic.	
292.	The solution must show the financing statement number as a hyperlink for State of Michigan users to see all information associated with the full filing record	
293.	The solution must allow State of Michigan users to click on any filing number returned for the secured party name search to see all information associated with the filing record.	
294.	<p>The solution must allow State of Michigan users to search for UCC-11 searches using all types of numbers that may be used to identify a search.</p> <p>Example, if a UCC-11 is assigned a search number and a work order number, State of Michigan users must be able to search by either number.</p>	
295.	<p>The solution must display the search criteria exactly as entered by the public user.</p> <p>Example, if an individual debtor name was searched, this State of Michigan user search must display the debtor's first name and surname in separate boxes. If only a surname was entered as search criteria, only the surname field will contain information.</p>	
296.	The solution must display whether the public user selected individual or organization for the debtor type.	

A	B	
Business Specification Number	Business Specification	NIST Family
	REQUIRED REQUIREMENTS SECTION 10: UCC Search and Filing Fees	
297.	The solution must allow the fee table to be editable by State of Michigan users, restricted by role-based security. This includes the ability to add/remove fee categories.	
298.	The solution must not charge a fee for, configured by State of Michigan Users: <ul style="list-style-type: none"> - UCC-11 Searches, by select users - Filings by select users 	
299.	The solution must have a shopping cart.	
300.	The solution must restrict the number of filings or searches in the shopping cart. Note: The number can be decided during discussions between State of Michigan and successful Contractor.	
301.	The solution must allow any combination of searches and filings in the shopping cart.	
302.	The solution must allow items to remain in the shopping cart for a defined number of days configurable by the State of Michigan, restricted by role-based security, before automatically deleting them.	
303.	The solution must allow a public user to select a payment type in the shopping cart.	
304.	The solution must allow one payment type to be selected. Payments may not be split between two types.	
305.	The solution must allow the public user to select one of the following payment types: <ul style="list-style-type: none"> - Billing account number - Credit or Debit Card 	
306.	If the public customer does not have a billing account associated with their user account, the solution must not display that payment type for selection from the shopping cart.	

A	B	
Business Specification Number	Business Specification	NIST Family
307.	The solution must prevent submission of a filing or search from the shopping cart if an error is received from CEPAS or CARS that causes payment to fail.	
	<p>REQUIRED REQUIREMENTS</p> <p><u>SECTION 11: Unique Identification Stamp</u></p>	
308.	The solution must automatically place a unique identification stamp on each filing (digital document and printed copy).	
309.	The solution unique identification stamp must be configurable/editable by the State of Michigan. Content details will be provided at a later time.	
310.	The solution must use the same unique identification stamp in both the test and production environment.	
311.	The solution must include a large unique watermark to distinguish filings created in the test environment from those created in the production environment.	
	<p>REQUIRED REQUIREMENTS</p> <p><u>SECTION 12: Filing Numbers</u></p>	
312.	<p>The solution must use a uniform enumeration schema that assigns a unique number to each filing record. The unique number must contain a check digit that is mathematically derived from or related to the other digits in the file number. This schema is set forth in MCL 440.9519.</p> <p>The solution must restart the sequence number at the beginning of each calendar year meaning 2022 becomes 2023 so the first filing of the new year would be 20230101000001-8.</p>	

A	B	
Business Specification Number	Business Specification	NIST Family
	The solution may restart the sequence each day meaning the system can begin each day with filing #1 i.e., 20220328000001-8.	
313.	The solution must use the same schema for all filing submission channels.	
314.	The solution must assign filing numbers in order regardless of submission channel. For example, the first document is received online, the second is XML, the third is mailed, the fourth is online. The first document must be 20220328000001-8, the XML second document is 20220328000002-7, the third mailed document is 20220328000003-6, and the online fourth document is 20220328000004-5.	
315.	The solution must use the same schema in both the test and production environments	
316.	The solution must not assign a sequence number if a filing is rejected, regardless of submission channel.	
317.	The solution must accept input of any existing filing number configuration through all channels. Exact configurations will be provided at a later time.	
REQUIRED REQUIREMENTS SECTION 13: Filing Attachments		
318.	The solution must allow uploading of attachments regardless of filing channel.	
319.	The solution must allow attachments up to 10 MB in size.	
320.	The solution must allow multiple files to be attached as long as the total size is 10 MB or less.	
321.	The solution must allow attachments in PDF and JPEG file formats. Additional formats may be determined at a later date.	
322.	The solution must allow the user to remove/delete a document after it has been attached but the filing has not been submitted.	

A	B	
Business Specification Number	Business Specification	NIST Family
323.	If an attachment is removed, the solution must allow the user to select and attach a different document.	
REQUIRED REQUIREMENTS SECTION 14: Storage of Filing Data and Images		
324.	The solution must create an electronic image of the filing.	
325.	The solution must create an electronic image in a format acceptable to FileNet (or similar image storage solution) regardless of input channel.	
326.	The solution must include any attachments submitted through any filing channel as part of the electronic filing image.	
327.	The solution must store data in the designated index and data fields for each filing regardless of input channel in compliance with IACA standards. Note: index and data fields will be provided later.	
328.	The solution must link the stored data to the electronic images regardless of data input channel.	
329.	The Contractor must provide a database dictionary including plain English descriptions of the database fields, the information contained in them, And the allowable number of characters for each field. The document must also indicate the character types (I.e., alpha, numeric, etc.) allowed in each field.	
330.	The solution must store the filing date and time as index data for the filing regardless of input channel.	
REQUIRED REQUIREMENTS SECTION 15: Delivery of Filings and Searches		
331.	The solution must allow, but not require, entry of an email address for the “Mail Acknowledgement Copy To” field.	
332.	The solution must store information if entered in the “Mail Acknowledgement Copy To” field.	

A	B	
Business Specification Number	Business Specification	NIST Family
333.	If an email address is provided, the solution must email a copy of the filing acknowledgement image to the provided email.	
334.	The solution must allow a different email to be entered for “Mail Acknowledgement Copy To” field for each filing even if they are processed in the same Work Order or Shopping Cart.	
335.	The solution must provide for electronic delivery of filings, filing acknowledgements, rejected filings, search reports, and search copies to an electronic mailbox which can only be accessed after the customer logs in to the system. This delivery must occur regardless of filing input channel.	
336.	The solution must send an automatic email to the filer upon completion of a filing or search. Email content to be configurable by the State of Michigan, restricted by role-based security.	
337.	The solution must allow customers or State of Michigan users to open and print all documents from the electronic delivery point (mailbox, submission history, whatever the term is).	
338.	The solution must allow customers or State of Michigan users to open and save/download all documents from the electronic delivery point.	
339.	The solution must make filing acknowledgements, filing images, filing rejection documents and UCC-11 search results available to the public user for 90 days including the date of electronic delivery. This availability must be the same for all filings regardless of input channel.	
340.	The solution must allow State of Michigan users access to view the public user’s filings, rejections and search results in their electronic delivery mailbox during the 90-day availability period.	
REQUIRED REQUIREMENTS		

A	B	
Business Specification Number	Business Specification	NIST Family
	<u>SECTION 16: Time and Filing Status Requirements</u>	
341.	The solution must consider 12:00:00 am to be the start of a day and 11:59:59 pm to be the end of a day. This solution must change filing status at this time.	
342.	The solution must allow filing statuses equal to active, lapsed, and inactive/expired or the equivalent.	
343.	The solution will allow UCC-1 Initial Financing Statements to be active for five (5) years.	
344.	<p>The solution may allow status times to be configurable based on type.</p> <ul style="list-style-type: none"> - Examples <ul style="list-style-type: none"> o UCC-1 Public Finance Initial Financing Statement to be active for 5 years o UCC-1 Transmitting Utility Initial Financing Statements to be active indefinitely 	
345.	The solution must display a lapse date of 12/31/9999 for Federal Estate Tax Liens and Transmitting Utility UCC filings or the Contractor must propose an alternative way to designate the lapse date of filings that are active indefinitely.	
	<p>REQUIRED REQUIREMENTS</p> <p><u>SECTION 17: Queries and Additional Reports</u></p>	
346.	<p>The solution must have an ad hoc query, restricted by role based security, that allows the State of Michigan users to find the following information, including, but not limited to:</p> <ul style="list-style-type: none"> - IP addresses <ul style="list-style-type: none"> o Retrieve IP addresses o Track and store when a public user account is created or modified o Location of where a UCC filing was submitted 	

A	B	
Business Specification Number	Business Specification	NIST Family
	<ul style="list-style-type: none"> - Filer account information - Filer account contact information - Filer account activity status (active/inactive) - Last login date for public and XML users - Retrieve filing information - Filing type and/or sub-type and/or sub-sub-type - Run query within a date range - Exportable 	
347.	The solution must provide a report which lists all deleted filings. Additional details of report contents will be provided at a later date.	
348.	The solution must allow access to reports and queries to be restricted by role-based security.	
349.	The solution must allow reports to be generated by the State of Michigan users with the following criteria, but not limited to: <ul style="list-style-type: none"> - Date range - Username 	
350.	The solution must allow multiple criteria to be used simultaneously to generate a report.	
351.	The solution must allow reports to be printed.	
352.	The solution must have a purge report.	
353.	The solution must provide a State of Michigan users production report that shows the amount of work completed per user. Additional details of report contents will be provided at a later date.	
354.	The solution must provide a report listing all filings for which an image has not been created and sent to FileNet (or similar image storage solution) with the below criteria, but not limited to: <ul style="list-style-type: none"> - Sortable columns - Column for filing channel - Column for election of specific filings which need images 	

A	B	
Business Specification Number	Business Specification	NIST Family
	Additional details of report contents will be provided at a later date.	
355.	The Contractor must provide a document that details what criteria is used to return results in each field on a report and how each report can be used.	
356.	The Contractor must provide samples of reports the application currently generates.	
357.	The solution must support up to 25 canned reports with the initial implementation.	
	<p>OPTIONAL REQUIREMENTS</p> <p><u>SECTION 17: Queries and Additional Reports</u></p>	
358.	The solution should include a column for selection of specific filings which need images recreated.	
359.	The solution should allow a single button to be clicked to regenerate images for all selected filings at once rather than having to recreate each image individually.	
	<p>REQUIRED REQUIREMENTS</p> <p><u>SECTION 18: Financial Requirements</u></p>	
360.	<p>The solution must provide a searchable/sortable financial reconciliation report that contains the following payment information, but is not limited to:</p> <ul style="list-style-type: none"> - displays all filings paid for by credit card - displays a status of payment such as accepted, pending, etc. <ul style="list-style-type: none"> o Provide clear, plain English definitions of each status which will appear on this report - displays all XML filings paid for by eCheck 	

A	B	
Business Specification Number	Business Specification	NIST Family
	<ul style="list-style-type: none"> - displays all filings paid for by billing account number - displays all filings paid for by CARS payment ID Additional details of report contents will be provided at a later date.	
361.	The solution must allow the financial reconciliation report for each payment channel to be generated at any time for a period of seven (7) years.	
362.	The solution must store payment information in a database table for seven (7) years.	
363.	The solution must store payment amount, service fee amount for credit card payments, payment date, payment confirmation ID, payment method, payment origin (i.e., online, XML), and user account who initiated the payment.	
364.	The solution must provide a way to link the payment to the specific filing(s) or search(es) it covers.	
365.	The solution must include a way to retrieve payment information from the State of Michigan user interface.	
366.	The solution must allow access to the financial information retrieval to be restricted by role-based security.	
367.	The solution must provide State of Michigan users a refund approval process and a way to issue payment refunds for credit card and registered eCheck payment types, restricted by role-based security.	
368.	The solution must require a review and approval process before a refund is issued.	
369.	The solution will implement multiple approvals based on the dollar amount of the refund. Details regarding the approval process will be provided at a later date.	
370.	The solution must store the following refund information for seven (7) years: <ul style="list-style-type: none"> - refund date 	

A	B	
Business Specification Number	Business Specification	NIST Family
	<ul style="list-style-type: none"> - refund amount - refund ID - how the refunded amount is tendered (check, credit card, etc.). 	
371.	The solution must allow State of Michigan users to access and retrieve refund information, restricted by role-based security.	
372.	The solution must charge a percentage-based credit card service fee, configurable by State of Michigan, restricted by role-based security.	
373.	The solution must charge the service fee for all credit and debit card purchases.	
374.	The solution must have a report that identifies the service fee charged per transaction.	
	<p>REQUIRED REQUIREMENTS</p> <p><u>SECTION 19: Output Products</u></p>	
375.	The solution must provide an opt-in feature for organizations to be notified by email if a UCC is filed listing them as a debtor.	
376.	The solution must produce output documents in PDF format.	
377.	<p>The Contractor must provide an output product document to include the following:</p> <ul style="list-style-type: none"> • Samples of final accepted documents • What transactions generate documents and what those documents are • When documents are printed • Where information included in the document is generated from. Example: the debtor first name on the output document is pulled from the debtor first name field. • Field length limitations 	

A	B	
Business Specification Number	Business Specification	NIST Family
	<ul style="list-style-type: none"> If any documents are printed in a batch file, time of day the file is printed and how the file is generated. <p>If automated emails are sent from the system, the document must include the content of each email and what triggers the email to be sent.</p>	
378.	The solution must make all output documents visible to State of Michigan users regardless of amount of time since filing or search was completed.	
379.	The solution must allow State of Michigan users to open and download output documents and print.	
380.	The solution must produce a debtor notice for each filing which names an individual as a debtor. This letter is required under MCL 440.9501(4).	
381.	<p>The solution must produce the debtor letter and copy of the filing image for all individual debtors named in:</p> <ul style="list-style-type: none"> - an initial UCC - Federal Tax Lien - State Tax Lien filing. - Unemployment Tax Lien 	
382.	The solution must produce the debtor letter for all individual debtors named in later action filings including but not limited to debtor add amendments.	
383.	The solution must generate and automatically print debtor letters daily as a batch job at a time specified by State of Michigan.	
384.	The solution must allow State of Michigan users to reprint a single debtor letter or entire file of debtor letters.	
385.	The Contractor must provide specific instructions on how to reprint the entire file of debtor letters.	

A	B	
Business Specification Number	Business Specification	NIST Family
386.	The solution must allow more than one day's letter file to be reprinted. This is especially important if the UCC printer is down for maintenance for multiple days.	
387.	The solution must create a transaction receipt. Content of the receipt will be provided at a later time.	
388.	The solution must create an acknowledgement packet containing filing type, sub-types and sub-sub- types. Note: if the filing is processed by UCC State of Michigan users, the acknowledgement packet must include a copy of the scanned image.	
389.	The solution must create an acknowledgement packet that shows filing type, sub-type, and sub-sub-type on acknowledgement copies, with required information as outlined by State of Michigan.	
390.	If filing type is UCC-1 Initial Financing Statement, the solution must display UCC-1 Initial Financing Statement on the acknowledgement copy.	
391.	If Transmitting Utility is selected, the solution must display UCC-1 Initial Financing Statement Transmitting Utility on the acknowledgement copy.	
392.	If Mobile Home is selected, the solution must display UCC-1 Initial Financing Statement Mobile Home on the acknowledgement copy.	
393.	If filing type is UCC-3 Termination, the solution must display UCC-3 Termination on the acknowledgement copy.	
394.	If the filing type is UCC-3 Continuation, the solution must display: <ul style="list-style-type: none"> - UCC-3 Continuation on the acknowledgement copy. - the new filing lapse date 	
395.	If the filing type is UCC-3 Assignment, the solution must display:	

A	B	
Business Specification Number	Business Specification	NIST Family
	<ul style="list-style-type: none"> - UCC-3 Assignment on the acknowledgement copy. - display the filing action Assignment - the assignee and assignor information - a collateral indicator for filings processed online. - Note: if the filing is processed by State of Michigan users, this indicator may show on the scanned document. - any text entered in the collateral field during online processing. 	
396.	<p>If the filing type is UCC-3 Amendment Party, the solution must display:</p> <ul style="list-style-type: none"> - UCC-3 Amendment Party on the acknowledgement copy - the amendment sub-sub-type (e.g., debtor add) - the added debtor name(s) and address(es) - changed debtor information - the deleted debtor name(s) - party(ies) and address(es) - changed secured party information - deleted secured party 	
397.	<p>If the filing type is UCC-3 Amendment Collateral, the solution must display:</p> <ul style="list-style-type: none"> - UCC-3 Amendment Collateral on the acknowledgement copy. - Collateral Add - Collateral Delete - Collateral Restate - display any text entered in the collateral box during online processing 	
398.	<p>If the filing type is UCC-5 Information Statement, the solution must display on the acknowledgement:</p> <ul style="list-style-type: none"> - UCC-5 Information Statement. - display the initial financing statement number 	

A	B	
Business Specification Number	Business Specification	NIST Family
	<ul style="list-style-type: none"> - the record information the UCC- 5 relates to (box 1b on paper form) on the acknowledgement copy. <ul style="list-style-type: none"> o Note: This information may be the initial financing statement number or a later action filing number. - one of the following selections that can be made by the filer: <ul style="list-style-type: none"> o Record is inaccurate o Record was wrongfully filed o Record filed by person not entitled to do so - Text entered from a free form text box that is part of the UCC-5 flow 	
399.	If the filing type is UCC-7 Affidavit of Fraudulent filing, the solution must display this on the acknowledgement copy. Note: UCC-7s may only be processed by State of Michigan users.	
	<p>REQUIRED REQUIREMENTS</p> <p><u>SECTION 20: XML</u></p>	
400.	The solution must allow for XML submittal of UCC filings.	
401.	The XML solution must adhere to IACA XML Specifications 4.0.	
402.	The Contractor must assist in creating XML filing implementation guide to be provided to Michigan’s XML filing customers.	
403.	The solution must allow attachments to be submitted via XML up to 10 MB.	
404.	The solution must allow filings to process with or without punctuation in data fields.	

A	B	
Business Specification Number	Business Specification	NIST Family
405.	The solution must provide XML processing errors in plain English. All error messages must be detailed enough to easily determine the problem and resolution.	
406.	The solution must allow submission of multiple assignment authorizing parties through XML.	
407.	The solution must allow multiple continuations to be submitted through the XML channel. Submission of multiple continuations via XML must follow the same requirements as other processing channels.	
	<p>REQUIRED REQUIREMENTS</p> <p><u>SECTION 21: Bulk Data and Images</u></p>	
408.	The solution must provide a method of bulk data and image file generation and electronic delivery.	
409.	The solution must allow customers to subscribe to receive the bulk data or image update file. Options for subscription length to be determined by State of Michigan.	
410.	The solution must make each database update file and image file available for download for a number of days from the date of delivery, determined by the State of Michigan.	
411.	The Contractor must create and provide to State of Michigan a document detailing the fields, field length, and field descriptions included in the bulk data files. This document will be provided to Michigan’s customers. Note: To be updated as needed by the Contractor.	
412.	The solution must create and deliver a data file, the full database file, containing all active UCC, state tax, and federal tax filings in the UCC database.	
413.	The solution must create the full database file on the 5 th of each month during non-peak times, i.e., 2:00 am EST	

A	B	
Business Specification Number	Business Specification	NIST Family
	(time to be decided by Contractor and State of Michigan at a later time)	
414.	The solution must create the full database file containing filings through the last day of the previous month.	
415.	The solution must allow purchase of the full database file on an as-ordered basis. No subscription is required, and customers may purchase the file at any time.	
416.	The solution must overwrite the full database file each time one is created meaning past files must not be available for download like the data update and image files.	
417.	The solution must allow download of the full database file at any time after the file has been made available and is purchased.	
418.	The solution must create and electronically deliver bulk data and image update files weekly, i.e., on Sundays at 2:00 am EST (time to be decided by Contractor and State of Michigan at a later time).	
419.	The data and images in the update files must be for a specific time frame (to be decided by Contractor and State of Michigan at a later time).	
420.	The solution must include the full Filing Officer Statement in the full database, data update, and image bulk files.	
421.	The solution must include the corrected debtor information, secured party information, filing type, lapse date, and/or filing status that was changed with the Filing Officer Statement in the full database and data update files.	
422.	The solution must include corrected images in the bulk image file.	
423.	The solution must provide all images in the update file in PDF format.	

A	B	
Business Specification Number	Business Specification	NIST Family
424.	The solution must provide a method for State of Michigan users to: <ul style="list-style-type: none"> - obtain copies of bulk data and image files - recreate the bulk data and image files - repost bulk data and image files 	
425.	The Contractor must provide a document detailing how to regenerate and deliver bulk data and image files.	
426.	The solution must allow the State of Michigan to edit/update/configure the bulk data/image agreement, restricted by role-based security.	
427.	The solution must require the public user to electronically accept an agreement to purchase bulk data and/or image files.	
428.	The solution must track user account, date and time of acceptance of agreement to purchase bulk data and/or image files.	
429.	The solution must provide a way for the State of Michigan user to export the purchase agreement acceptance information in Word, Excel and PDF formats, restricted by role-based security.	
430.	The solution must require re-acceptance of the bulk data/image agreement every 2 years and each time the agreement is updated.	
431.	The solution must provide a PDF version of the data/image agreement for public users to download.	
432.	The solution must require payment for bulk data or image files by billing account number or credit card.	
433.	The solution must exclude information entered in the Mail To: fields from the bulk data update and full database files.	
	OPTIONAL REQUIREMENTS <u>SECTION 21: Bulk Data and Images</u>	

A	B	
Business Specification Number	Business Specification	NIST Family
434.	The solution should include deleted filings in the full database, data update and image bulk files with an indicator they were deleted.	
435.	The Contractor should provide information about the deleted filing indicator in the document with other file specifications that will be provided to customers.	
<p align="center">REQUIRED REQUIREMENTS</p> <p align="center"><u>SECTION 22: Retention</u></p>		
436.	<p>The solution UCC-1 sub-type must determine lapse date.</p> <ul style="list-style-type: none"> - UCC-1 Initial Financing Statement <ul style="list-style-type: none"> o Initial Financing Statement <ul style="list-style-type: none"> ▪ Lapse date five (5) years from the filing date o Manufactured Home <ul style="list-style-type: none"> ▪ Lapse date 30 years from the filing date o Transmitting Utility <ul style="list-style-type: none"> ▪ Lapse date is indefinite from the date of filing ▪ Public Finance Lapse date is five (5) years from the filing date 	
437.	The solution must be in, and maintain, compliance with MDOS and State of Michigan retention schedules.	
438.	The solution must allow filing records to be searched using a UCC-11 search request for 1 year past lapse date through the public users site.	
439.	The Contractor must provide, and maintain, documentation of how filings are maintained in the database after expiration but before being purged at the end of the retention period. Documentation to specify	

A	B	
Business Specification Number	Business Specification	NIST Family
	what table expired filings are moved to if they are moved.	
440.	The Contractor must provide, and maintain, documentation of how filings are purged from the database at the end of the retention period.	
441.	The solution must be in, and maintain, compliance with retention of information identified in SOM Technical Standard 1340.00.040.01 Audit and Accountability Standard.	
442.	The Contractor must comply, and maintain compliance, with the retention of information in the solution meets the requirements of SOM Records Retention and Disposal Schedule, General Schedule 9 – Technology Systems Records, GS-IT-0508 System Audit Records.	
443.	The solution must automatically purge documents (filings and images) from the database, in compliance with State of Michigan retention and disposal schedules.	
444.	The solution must allow State of Michigan users to configure the frequency of the automatic purge schedule, restricted by role-based security.	
	REQUIRED REQUIREMENTS <u>SECTION 23: Data Migration and Environments</u>	
445.	The solution must provide a simple way to migrate production data back to lower environments.	
446.	The Contractor must provide, and maintain, technical documentation explaining the data migration process among environments.	
447.	The solution must not overwrite user accounts created in the lower environments when production data is migrated. The preferred solution would not require user accounts to be copied as part of the migration. Note: this	

A	B	
Business Specification Number	Business Specification	NIST Family
	requirement is due to different security permissions being allowed in lower environments versus production.	
448.	The solution must overwrite any data, excluding user accounts, created solely in the test environment when the production data is migrated back.	
449.	The Contractor must provide, and maintain, a Data Migration Plan (and conversion).	
450.	The Contractor must migrate all UCC data and images from the existing UCC system to the modernized UCC system.	
451.	The Contractor must provide the database schema/data models.	
452.	The Contractor must assess current UCC data and provide documentation related to data cleansing and discuss with MDOS each data type they believe requires cleansing.	
453.	The Contractor, upon agreement from MDOS, may perform automated data cleansing and provide assistance to State of Michigan users related to data cleansing that must be performed manually.	
454.	The Contractor must make the STG/DEV and UAT environments mirror copies of the production environment and maintain through the life of the contract.	
455.	The solution must not revert previously made changes in STG/DEV, UAT and PRD, unless intentional to correct a defect. (Assured by Contractor conducting regression testing)	
456.	The solution STG/DEV and UAT environments must include a portal for XML filers to test their filing configurations. This portal must be available 24x7x365.	
457.	The Contractor must provide an XML portal for State of Michigan user to submit filings to the STG/DEV and	

A	B	
Business Specification Number	Business Specification	NIST Family
	UAT environments. This portal must be available 24x7x365.	
	REQUIRED REQUIREMENTS <u>SECTION 24: General Technical Requirements</u>	
458.	The system must electronically deliver: <ul style="list-style-type: none"> - All filings - Rejections - UCC-11 Search results 	
459.	The Contractor must create a splash page to be displayed when the system is down, configurable by State of Michigan restricted by role-based security.	
460.	The solution must display the “through date” of filings on the non-logged in homepage, text must be configurable by State of Michigan.	
461.	The solution must display messages to all UCC customers on the non-logged and logged in homepages, configurable/editable/add and remove by State of Michigan.	
462.	The solution must allow a free-form text entry box for State of Michigan user to enter the message text, character limit to be discussed once Contract is executed. Note: if the logged-in and non-logged in messages are displayed differently, the character limit may be different for each location.	
463.	The solution must allow State of Michigan user to select a date range (including future dates) during which the message must be posted. The solution must hold this message and post on the date selected without manual intervention.	
464.	The solution must provide online filing instructions for, including but not limited to, each filing type, sub-type and sub-sub-type; bulk data or image purchase;	

A	B	
Business Specification Number	Business Specification	NIST Family
	obtaining filing acknowledgements and search results; shopping cart; etc. The intent is to have access to instructions from every screen in the filing or search flow.	
465.	The solution must allow State of Michigan users to edit all instructions and update them as necessary, restricted by role-based security.	
466.	The solution must prevent navigation from one screen in the filing or search flow to the next screen if a required field is not complete.	
467.	The solution must display all error messages in plain English to explain which field(s) is not complete.	
468.	The solution must display all error messages written in plain English. Note: State of Michigan must provide and/or approve verbiage for error messages during solution development.	
469.	The Contractor must provide a document that contains: <ul style="list-style-type: none"> - Error message <ul style="list-style-type: none"> o How the error shows to the user - Meaning of error messages in plain English - How to resolve error (i.e. close then reopen browser, contact a phone number etc.) 	
470.	The solution must allow State of Michigan configuration of all columns shown on informational tables and all search results. This configuration would allow State of Michigan users to add or remove columns of information to ensure the table displays the information the State of Michigan users most needs.	
471.	The solution must allow all tables to be sortable by columns. (i.e. ascending, descending, customer name	

A	B	
Business Specification Number	Business Specification	NIST Family
	column sorted alphabetically or reversed, account status column sorted by status type)	
472.	The solution must allow State of Michigan users to do a keyword search in tables.	
473.	The solution must allow State of Michigan users to print all documents and reports.	
474.	The solution must allow State of Michigan users to print generated notifications/letters individually and as a batch. If batch printing is desired, allow State of Michigan user functionality to select multiple items (i.e. check box).	
475.	The solution must allow all documents generated, including reports, to be exported to Word, Excel, CSV, and PDF. If both Excel and CSV are not available, CSV would be preferred.	
476.	The solution must have filter capabilities for all tables.	
477.	Contractor must renew licenses, update security patches, maintain access keys, etc. that may be associated with third-party components or open-source components.	
REQUIRED REQUIREMENTS SECTION 25: Interfaces		
478.	The solution must allow credit card payments when redirected to CEPAS.	
479.	The solution must interface with the CEPAS payment gateway using an API for registered eCheck payments.	
480.	The solution must interface with CARS the State of Michigan payment processing system, using an API.	

A	B	
Business Specification Number	Business Specification	NIST Family
481.	<p>The Contractor must provide a technical interface document to detail how the connection between the UCC system, CARS, FileNet (or similar image storage solution) and CEPAS (include credit cards and registered eCheck) functions.</p> <p>Note: This document must detail troubleshooting options, error messages, status codes and their definitions in plain English the document must also include any additional software State of Michigan will be required to purchase to interface with programs detailed above.</p>	
482.	<p>The solution must provide an error message written in plain English if the connection with CEPAS is not available, error messages to be approved by State of Michigan.</p>	
483.	<p>The solution must interface with FileNet (or similar image storage solution), using an API if FileNet is used.</p>	
484.	<p>The solution must create and send PDF image files to FileNet (or similar image storage solution).</p>	
485.	<p>If the solution uses FileNet for the image storage solution, the solution must be FileNet version agnostic.</p>	
486.	<p>The solution must interface with CARS, using an API, to validate UCC billing accounts and payment IDs.</p>	

SCHEDULE B - PRICING

1. Licensing Cost

Table A – Non-Subscription License Model

Licensed Product Name	Perpetual Licensing – One Time Cost	Monthly Hosting Fees including tiered pricing – First Year
RegSys	\$500,000.00	\$4,587.66

Licensing and Hosting costs will be paid after installation, configuration, and State testing and acceptance of the Solution.

2. Implementation Fees. All costs associated with Implementation Services are included below (e.g. configuration, customization, migration, integration, testing, etc.) (the “**Implementation Fees**”). All costs are firm fixed.

Payment will not be released until Milestone is delivered and approved by the State Program Managers.

The following timeline remains tentative due to the outputs during the Evaluation & Feedback stage of each release.

Caveats for this project timeline:

- The milestone completion date is dependent on getting a detailed understanding of the solution integration points and other requirements.
 - As an example, the Tax and State Filing integration and the CEPAS integration will have expected variability in the timeline. ISC needs a to analyze the detailed requirements for the integrations and create a design and plan to implement.
- The milestone completion date is dependent on the data quality and quantity of different types of data to be migrated. Both these considerations can have a meaningful impact on data conversion and migration.
- The milestone completion date is dependent on the detailed requirements for the configurable website content. This functionality needs to be further understood to confirm it reflects our existing functionality.
- The milestone completion date is dependent on the State’s availability and the availability of relevant 3rd party vendors during the project.

MILESTONE COMPLETION DATES	INVOICING MODEL (\$)	FINANCIAL MODEL (\$)	PLANNED DELIVERABLES	
11/1/2023			PROJECT START DATE	
12/3/2023	\$35,000.00	\$70,000.00	PROJECT KICKOFF	Project Kickoff, determine lifecycle management tool, determine team norms, initial SUITE project tailoring training
				Dev/ UAT Environment Setup/Infrastructure [Create & validate Test environments, Network Diagram Design For Test Environment] [SSP Stages 1.0-5.0]
				Login Creation in DevOps
				CI/CD Pipeline Creation
				Requirement Analysis/ Design Phase [Discovery and Validation sessions, Requirement Validation Document, Role-Based Security Matrix, Design Document, Detailed Requirements]
	\$35,000.00		DATA MIGRATION	Analyze and categorize source data
				Identify data quality issues
				Map source data to RegSys Database
				Data cleansing and correction action planning
				Data Migration Run planning
01/21/2024	\$100,000.00	\$140,000.00	CUSTOMER PORTAL	ONLINE FORMS
				System Configuration

				Define B2B Interfaces
				FileNet Integration
				CEPAS Integration
				UAT Release - (UCC Filing) - SOM Testing
				Conduct Data Migration
				Run-1
				Perform Test Data Migration - Data Only
				Perform Test Data Migration - Image Only
				Review and Analyze Data Migration Results
				Data Migration Testing - Internal QA / Bug Fixing
				Data Migration Testing- SOM / Bug Fixing
				DATA MIGRATION
				\$40,000.00
				Search Logic
				CARS Integration
				Other Service Integration
				CUSTOMER PORTAL
				Paper based configuration
				Task configuration
				All back-office configuration
				Report Configuration
				Address Lookup Integration (Client to provide API)
				Search Logic
				BACK OFFICE
				\$60,000.00
				\$140,000.00
				2/25/2024

				UAT Build Release - SOM Testing
			DATA MIGRATION	Conduct Data Migration
				Run-2
				Perform Test Data Migration - Data Only
				Perform Test Data Migration - Image Only
				Review and Analyze Data Migration Results
				Data Migration Testing - Internal QA / Bug Fixing
				Data Migration Testing- SOM / Bug Fixing
	\$40,000.00			
5/12/2024			CUSTOMER PORTAL	B2B Environment Configuration (UAT)
				Customer Portal UAT Testing - SOM Testing/Bug Fixing
			BACK OFFICE	Content Management for customer portal
				Content Management for customer portal - UAT SOM Testing
	\$40,000.00			
5/12/2024			DATA MIGRATION	Conduct Data Migration
				Run-3
				Perform Test Data Migration - Data Only
				Perform Test Data Migration - Image Only
				Review and Analyze Data Migration Results
	\$60,000.00			
		\$140,000.00		

				Data Migration Testing - Internal QA / Bug Fixing
				Data Migration Testing- SOM / Bug Fixing
				Conduct Data Migration
				Run-4
				Perform Test Data Migration - Data Only
				Perform Test Data Migration - Image Only
				Review and Analyze Data Migration Results
				Data Migration Testing - Internal QA / Bug Fixing
				Data Migration Testing- SOM / Bug Fixing
				Conduct Data Migration
				Run-5 - FINAL
				Perform Test Data Migration - Data Only
				Perform Test Data Migration - Image Only
				Review and Analyze Data Migration Results
				Data Migration Testing - Internal QA / Bug Fixing
				Data Migration Testing- SOM / Bug Fixing
8/4/2024	\$70,000.00	\$140,000.00	DATA MIGRATION	

	\$70,000.00		RELEASE ACTIVITIES	System and User Documentation [Test Plan, Test Scenarios, Requirements traceability matrix, Test Results Report, Training Documentation & User Manuals, Product stabilization, Solution and Testing Documents, Technical Baseline document with final configurations, Training Plan]
9/15/2024	\$35,000.00	\$70,000.00	RELEASE ACTIVITIES	Full Integration/Regression Testing- Internal [SSP Stage 6.0 Risk Assessment SSP Stage 7.0 POAMs]
				Pen Testing/ Bug Fixing
				Load/Performance Testing /Bug Fixing
				User Training [Final Training Documentation]
9/16/2024			RELEASE ACTIVITIES	SOM – End-to-End UAT Testing Begins
10/13/2024	\$35,000.00		RELEASE ACTIVITIES	SOM – End-to-End UAT Testing Ends [Final Test Results Report] [SSP Authority to Operate (ATO)]
				Sign Off [Final Acceptance, Create & validate Production environments, Network Diagram Design for Production, Go-Live Plan]
10/31/2024	\$700,000.00	\$700,000.00		GO LIVE

			<p align="center">POST- PRODUCTION ACTIVITIES</p>	<p>Post-Production Warranty [Complete SSP POAMs. Resolve configuration issues that were deemed low priority and not preventing Go-Live.] Post Implementation and Production Support Service [Ongoing after Final Acceptance. Solution configuration adjustment as needed. Complete SSP POAMs.]</p>
--	--	--	--	---

3. Year over Year Costs

Initial Term Contract Pricing Per Year	Year 1	Year 2	Year 3	Year 4	Year 5	Total of 5 Years
Implementation	\$1,400,000.00					\$1,400,000.00
Hosting Fees	\$46,000.00	\$55,000.00	\$55,000.00	\$61,000.00	\$61,000.00	\$278,000.00
Licensing Fee	\$500,000.00					\$500,000.00
Maintenance & Support	\$0.00	\$265,000.00	\$270,000.00	\$278,000.00	\$285,000.00	\$1,098,000.00
TOTAL	\$1,946,000.00	\$320,000.00	\$325,000.00	\$339,000.00	\$346,000.00	\$3,276,000.00
Year over Year %			1.6%	4.3%	2.1%	

Optional Pricing Contract Pricing Per Year	Year 6	Year 7	Year 8	Year 9	Year 10	Total of 10 Years
Hosting Fees	\$61,000.00	\$66,000.00	\$66,000.00	\$66,000.00	\$72,000.00	\$609,000.00
Maintenance & Support	\$295,000.00	\$305,000.00	\$310,000.00	\$315,000.00	\$325,000.00	\$2,648,000.00
TOTAL	\$356,000.00	\$371,000.00	\$376,000.00	\$381,000.00	\$397,000.00	\$5,157,000.00

Year over Year %	2.9%	4.2%	1.3%	1.3%	4.2%
-------------------------	-------------	-------------	-------------	-------------	-------------

Contractor will be paid on a monthly basis after Go Live for maintenance, support and hosting.

4. Postproduction Warranty. The Contractor must provide a 90 calendar days postproduction warranty at no cost to the State. The postproduction warranty will meet all requirements of the contract, including all Support Services identified in Schedule D.

5. Rate Card for Ancillary Professional Services.

Resource	On-Site Hourly Rate
Quality Assurance Analyst	\$89
Quality Assurance Analyst, Senior	\$110
Infrastructure Analyst	\$107
Programmer/Systems Analyst	\$104
Senior Programmer Analyst	\$126
Intermediate Data Base Administrator	\$123
Intermediate Business Analyst	\$124
Senior Business Analyst	\$134
Information Security Architect, Application Architect	\$141
Project Manager	\$144
Principal Solutions Architect	\$171
Director, Cybersecurity	\$210

Fixed-price hourly-rate rate card for ancillary professional services (e.g. future enhancement configuration services) broken down by role (e.g. Solution design architect). Rates are fixed for the full term of the Contract.

6. Additional Pricing Terms

The Contractor is encouraged to offer quick payment terms. The number of days must not include processing time for payment to be received by the Contractor's financial institution.

Quick payment terms: _____N/A_____ % discount off invoice if paid within ___N/A_____ days after receipt of invoice.

If Contractor reduces its prices, or offers a lower price to any other entity, private or public, for any of the software or services during the term of this Contract, the State shall have the immediate benefit of such lower prices for new purchases. Contractor shall send notice to the State's Contract Administrator with the reduced prices within fifteen (15) Business Days of the reduction taking effect.

Ordering

Authorizing Document

The appropriate authorizing document for the Contract will be Delivery Order.

Travel and Expenses

The State does not pay for overtime or travel expenses.

Information Services Corporation (ISC)

SCHEDULE C - INSURANCE REQUIREMENTS

MDOS Uniform Commercial Code (UCC) System

MA 230000001706

1. General Requirements. Contractor, at its sole expense, must maintain the insurance coverage as specified herein for the duration of the Term. Minimum limits may be satisfied by any combination of primary liability, umbrella or excess liability, and self-insurance coverage. To the extent damages are covered by any required insurance, Contractor waives all rights against the State for such damages. Failure to maintain required insurance does not limit this waiver.

2. Qualification of Insurers. Except for self-insured coverage, all policies must be written by an insurer with an A.M. Best rating of A- VII or higher unless otherwise approved by DTMB Enterprise Risk Management.

3. Primary and Non-Contributory Coverage. All policies for which the State of Michigan is required to be named as an additional insured must be on a primary and non-contributory basis.

4. Claims-Made Coverage. If any required policies provide claims-made coverage, Contractor must:

a. Maintain coverage and provide evidence of coverage for at least 3 years after the later of the expiration or termination of the Contract or the completion of all its duties under the Contract;

b. Purchase extended reporting coverage for a minimum of 3 years after completion of work if coverage is cancelled or not renewed, and not replaced with another claims-made policy form with a retroactive date prior to the Effective Date of this Contract.

5. Proof of Insurance.

a. Insurance certificates showing evidence of coverage as required herein must be submitted to DTMB-RiskManagement@michigan.gov within 10 days of the contract execution date.

- b. Renewal insurance certificates must be provided on annual basis or as otherwise commensurate with the effective dates of coverage for any insurance required herein.
- c. Insurance certificates must be in the form of a standard ACORD Insurance Certificate unless otherwise approved by DTMB Enterprise Risk Management.
- d. All insurance certificates must clearly identify the Contract Number (e.g., notated under the Description of Operations on an ACORD form).
- e. The State may require additional proofs of insurance or solvency, including but not limited to policy declarations, policy endorsements, policy schedules, self-insured certification/authorization, and balance sheets.
- f. In the event any required coverage is cancelled or not renewed, Contractor must provide written notice to DTMB Enterprise Risk Management no later than 5 business days following such cancellation or nonrenewal.

6. Subcontractors. Contractor is responsible for ensuring its subcontractors carry and maintain insurance coverage.

7. Limits of Coverage & Specific Endorsements.

Required Limits	Additional Requirements
Commercial General Liability Insurance	
Minimum Limits: \$1,000,000 Each Occurrence \$1,000,000 Personal & Advertising Injury \$2,000,000 Products/Completed Operations \$2,000,000 General Aggregate	Contractor must have their policy endorsed to add “the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents” as additional insureds using endorsement CG 20 10 11 85, or both CG 20 10 12 19 and CG 20 37 12 19.
Automobile Liability Insurance	
If a motor vehicle is used in relation to the Contractor's performance, the Contractor must have vehicle liability insurance on the motor vehicle for bodily injury and property damage as required by law.	

Required Limits	Additional Requirements
Workers' Compensation Insurance	
Minimum Limits: Coverage according to applicable laws governing work activities.	Waiver of subrogation, except where waiver is prohibited by law.
Employers Liability Insurance	
Minimum Limits: \$500,000 Each Accident \$500,000 Each Employee by Disease \$500,000 Aggregate Disease	
Privacy and Security Liability (Cyber Liability) Insurance	
Minimum Limits: \$1,000,000 Each Occurrence \$1,000,000 Annual Aggregate	Contractor must have their policy cover information security and privacy liability, privacy notification costs, regulatory defense and penalties, and website media content liability.

8. Non-Waiver. This Schedule C is not intended to and is not to be construed in any manner as waiving, restricting or limiting the liability of either party for any obligations under this Contract, including any provisions hereof requiring Contractor to indemnify, defend and hold harmless the State.

SCHEDULE D – SERVICE LEVEL AGREEMENT

IF THE SOFTWARE IS CONTRACTOR HOSTED, then the following applies:

1. For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this **Schedule** shall have the respective meanings given to them in the Contract Terms and Conditions. **“Actual Uptime”** means the total minutes in the Service Period that the Hosted Services are Available.

“Availability” has the meaning set forth in **Section 2.1**.

“Availability Requirement” has the meaning set forth in **Section 2.1**.

“Available” has the meaning set forth in **Section 2.1**.

“Contact List” means a current list of Contractor contacts and telephone numbers set forth in the attached **Schedule D – Attachment 1** to this Schedule to enable the State to escalate its Support Requests, including: (a) the first person to contact; and (b) the persons in successively more qualified or experienced positions to provide the support sought.

“Corrective Action Plan” has the meaning set forth in **Section 3.9**.

“Critical Service Error” has the meaning set forth in **Section 3.5**.

“Exceptions” has the meaning set forth in **Section 2.2**.

“High Service Error” has the meaning set forth in **Section 3.5**.

“Low Service Error” has the meaning set forth in **Section 3.5**.

“Medium Service Error” has the meaning set forth in **Section 3.5**.

“Resolve” has the meaning set forth in **Section 3.6**.

“RPO” or **“Recovery Point Objective”** means the maximum amount of potential data loss in the event of a disaster.

“RTO” or **“Recovery Time Objective”** means the maximum period of time to fully restore the Hosted Services in the case of a disaster.

“**Scheduled Downtime**” has the meaning set forth in **Section 2.3**.

“**Scheduled Uptime**” means the total minutes in the Service Period.

“**Service Availability Credits**” has the meaning set forth in **Section 2.6(a)**.

“**Service Error**” means any failure of any Hosted Service to be Available or otherwise perform in accordance with this Schedule.

“**Service Level Credits**” has the meaning set forth in **Section 3.8**.

“**Service Level Failure**” means a failure to perform the Software Support Services fully in compliance with the Support Service Level Requirements.

“**Service Period**” has the meaning set forth in **Section 2.1**.

“**Software Support Services**” has the meaning set forth in **Section 3**.

“**State Systems**” means the information technology infrastructure, including the computers, software, databases, electronic systems (including database management systems) and networks, of the State or any of its designees.

“**Support Hours**” means Monday – Friday, 8:00am to 5:00pm, Eastern Standard Time.

“**Support Request**” has the meaning set forth in **Section 3.5**.

“**Support Service Level Requirements**” has the meaning set forth in **Section 3.4**.

2. Service Availability and Service Availability Credits.

2.1 Availability Requirement. Contractor will make the Hosted Services and Software Available, as measured over the course of each calendar month during the Term and any additional periods during which Contractor does or is required to perform any Hosted Services (each such calendar month, a “**Service Period**”), at least 99.98% of the time, excluding only the time the Hosted Services are not Available solely as a result of one or more Exceptions (the “**Availability Requirement**”). “**Available**” means the Hosted Services and Software are available and operable for access and use by the State and its Authorized Users over the Internet in material conformity with the Contract. “**Availability**” has a correlative meaning. The Hosted Services and Software are not considered Available in the event of a material performance degradation or inoperability of the Hosted Services and Software, in whole or in part. The Availability

Requirement will be calculated for the Service Period as follows: (Actual Uptime – Total Minutes in Service Period Hosted Services or Software are not Available Due to an Exception) ÷ (Scheduled Uptime – Total Minutes in Service Period Hosted Services or Software are not Available Due to an Exception) x 100 = Availability.

2.2 Exceptions. No period of Hosted Services degradation or inoperability will be included in calculating Availability to the extent that such downtime or degradation is due to any of the following (“**Exceptions**”):

- (a) Failures of the State’s or its Authorized Users’ internet connectivity;
- (b) Scheduled Downtime as set forth in **Section 2.3.**

2.3 Scheduled Downtime. Contractor must notify the State at least ten (10) business days in advance of all scheduled outages of the Hosted Services or Software in whole or in part (“**Scheduled Downtime**”). All such scheduled outages will: (a) last no longer than five (5) hours; (b) be scheduled between the hours of 12:00 a.m. and 5:00 a.m., Eastern Time; and (c) occur no more frequently than once per week; provided that Contractor may request the State to approve in writing extensions of Scheduled Downtime above five (5) hours, and such approval by the State may not be unreasonably withheld or delayed.

2.4 Software Response Time. Software response time, defined as the interval from the time the end user sends a transaction to the time a visual confirmation of transaction completion is received, must be less than two (2) seconds for 98% of all transactions. Unacceptable response times shall be considered to make the Software unavailable and will count against the Availability Requirement.

2.5 Service Availability Reports. Within fifteen (15) days after the end of each Service Period, Contractor will provide to the State a report describing the Availability and other performance of the Hosted Services and Software during that calendar month as compared to the Availability Requirement. The report must be in electronic or such other form as the State may approve in writing and shall include, at a minimum: (a) the actual performance of the Hosted Services and Software relative to the Availability Requirement; and (b) if Hosted Service performance has failed in any respect to meet or exceed the Availability Requirement during the reporting period, a description in sufficient detail to inform the State of the cause of such failure and the corrective actions the Contractor has taken and will take to ensure that the Availability Requirement are fully met.

2.6 Remedies for Service Availability Failures.

(a) If the actual Availability of the Hosted Services and Software is less than the Availability Requirement for any Service Period, such failure will constitute a Service Error for which Contractor will issue to the State the following credits on the fees payable for Hosted Services and Software provided during the Service Period (“**Service Availability Credits**”):

Availability	Credit of Fees
≥99.98%	None
<99.98% but ≥99.0%	15%
<99.0% but ≥95.0%	50%
<95.0%	100%

(b) Any Service Availability Credits due under this **Section 2.6** will be applied in accordance with payment terms of the Contract.

(c) If the actual Availability of the Hosted Services and Software is less than the Availability Requirement in any two (2) of four (4) consecutive Service Periods, then, in addition to all other remedies available to the State, the State may terminate the Contract on written notice to Contractor with no liability, obligation or penalty to the State by reason of such termination.

3. Support and Maintenance Services. Contractor will provide IT Environment Service and Software maintenance and support services (collectively, “**Software Support Services**”) in accordance with the provisions of this **Section 3**. The Software Support Services are included in the Services, and Contractor may not assess any additional fees, costs or charges for such Software Support Services.

3.1 Support Service Responsibilities. Contractor will:

- (a) correct all Service Errors in accordance with the Support Service Level Requirements, including by providing defect repair, programming corrections and remedial programming;
- (b) provide unlimited telephone support, Monday – Friday, 8:00am to 5:00pm, Eastern Standard Time.
- (c) provide unlimited online support, Monday – Friday, 8:00am to 5:00pm, Eastern Standard Time;

(d) provide online access to technical support bulletins and other user support information and forums, to the full extent Contractor makes such resources available to its other customers; and

(e) respond to and Resolve Support Requests as specified in this **Section 3.**

3.2 Service Monitoring and Management. Contractor will continuously monitor and manage the Hosted Services and Software to optimize Availability that meets or exceeds the Availability Requirement. Such monitoring and management includes:

(a) proactively monitoring on a twenty-four (24) hour by seven (7) day basis all Hosted Service functions, servers, firewall and other components of Hosted Service security;

(b) if such monitoring identifies, or Contractor otherwise becomes aware of, any circumstance that is reasonably likely to threaten the Availability of the Hosted Service, taking all necessary and reasonable remedial measures to promptly eliminate such threat and ensure full Availability; and

(c) if Contractor receives knowledge that the Hosted Service or any Hosted Service function or component is not Available (including by written notice from the State pursuant to the procedures set forth herein):

(i) confirming (or disconfirming) the outage by a direct check of the associated facility or facilities;

(ii) If Contractor's facility check in accordance with clause (i) above confirms a Hosted Service outage in whole or in part: (A) notifying the State in writing pursuant to the procedures set forth herein that an outage has occurred, providing such details as may be available, including a Contractor trouble ticket number, if appropriate, and time of outage; and (B) working all problems causing and caused by the outage until they are Resolved as Critical Service Errors in accordance with the Support Request Classification set forth in **Section 3.5 and 3.6**, or, if determined to be an internet provider problem, open a trouble ticket with the internet provider; and

(iii) Notifying the State in writing that Contractor has fully corrected the outage and any related problems, along with any pertinent findings or action taken to close the trouble ticket.

3.3 Service Maintenance. Contractor will continuously maintain the Hosted Services and Software to optimize Availability that meets or exceeds the

Availability Requirement. Such maintenance services include providing to the State and its Authorized Users:

- (a) all updates, bug fixes, enhancements, Maintenance Releases, New Versions and other improvements to the Hosted Services and Software, including the Software, that Contractor provides at no additional charge to its other similarly situated customers; provided that Contractor shall consult with the State and is required to receive State approval prior to modifying or upgrading Hosted Services and Software, including Maintenance Releases and New Versions of Software; and
- (b) all such services and repairs as are required to maintain the Hosted Services and Software or are ancillary, necessary or otherwise related to the State’s or its Authorized Users’ access to or use of the Hosted Services and Software, so that the Hosted Services and Software operate properly in accordance with the Contract and this Schedule.

3.4 Support Service Level Requirements. Contractor will correct all Service Errors and respond to and Resolve all Support Requests in accordance with the required times and other terms and conditions set forth in this **Section 3 (“Support Service Level Requirements”)**, and the Contract.

3.5 Support Requests. The State will classify its requests for Service Error corrections in accordance with the descriptions set forth in the chart below (each a “**Support Request**”), with the classification to be determined by a State Program Manager. Within 14 days of Resolution of a Support Request, Contractor may request reclassification of a Support Request solely for the purposes of adjusting the amount of any Service Level Credits that may have been assessed with respect to the applicable Support Request, subject to the State’s final determination. The State will notify Contractor of Support Requests by email, telephone or such other means as the parties may hereafter agree to in writing.

Support Request Classification	Description:
Critical Service Error	<ul style="list-style-type: none"> • Issue affecting entire system or single critical production function;

Support Request Classification	Description: Any Service Error Comprising or Causing any of the Following Events or Effects
	<ul style="list-style-type: none"> • System down or operating in materially degraded state; • Data integrity at risk; • Declared a Critical Support Request by the State; or • Widespread access interruptions.
High Service Error	<ul style="list-style-type: none"> • Primary component failure that materially impairs its performance; or • Data entry or access is materially impaired on a limited basis.
Medium Service Error	<ul style="list-style-type: none"> • IT Environment Services and Software is operating with minor issues, including those that may be addressable with an acceptable (as determined by the State) temporary work around.
Low Service Error	<ul style="list-style-type: none"> • Request for assistance, information, or services that are routine in nature.

3.6 Response and Resolution Time Service Levels. Response and Resolution times will be measured from the time Contractor receives a Support Request until the respective times Contractor has (i) responded to, in the case of response time and (ii) Resolved such Support Request, in the case of Resolution time. **“Resolve”** (including **“Resolved”**, **“Resolution”** and correlative capitalized terms) means that, as to any Service Error, Contractor has provided the State the corresponding Service Error correction and the State has confirmed in writing

such correction and its acceptance thereof. Contractor will respond to and Resolve all Service Errors within the following times based on the severity of the Service Error:

Support Request Classification	Service Level Metric (Required Response Time)	Service Level Metric (Required Resolution Time)	Service Level Credits (For Failure to Respond to any Support Request Within the Corresponding Response Time)	Service Level Credits (For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time)
Critical Service Error	Thirty (30) minutes First Contact: via phone or collaboration platform. The Response Time commences when Service Provider personnel respond either through a return phone call, collaboration platform or placing a comment on Service Now. Autogenerated responses from a ticketing system are	Four (4) hours If the Contractor Resolves the Support Request by way of a work-around accepted in writing by the State, the support classification assessment will be reduced to a High Service Error.	Five percent (5%) of the Fees for the month in which the initial Service Level Failure begins and five percent (5%) of such monthly Fees for each additional hour or portion thereof that the corresponding Service Error is not responded to within the required response time.	Five percent (5%) of the Fees for the month in which the initial Service Level Failure begins and five percent (5%) of such monthly Fees for the first additional hour or portion thereof that the corresponding Service Error remains un-Resolved, which amount will thereafter double for each additional one-hour increment.

Support Request Classification	Service Level Metric (Required Response Time)	Service Level Metric (Required Resolution Time)	Service Level Credits (For Failure to Respond to any Support Request Within the Corresponding Response Time)	Service Level Credits (For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time)
	<p>not considered responses for the purposes of calculating Response Time.</p> <p>Updates: hourly during support hours. May be via telephone, collaboration platform, or email.</p>			
High Service Error	One (1) hour First contact for new issue: via phone, collaboration platform, email or comment in Support Request ticketing system that	Five (5) hours for a new issue or, where applicable, the State's written acceptance of a Critical Service Error work-around, within	Three percent (3%) of the Fees for the month in which the initial Service Level Failure begins and three percent (3%) of such monthly Fees for each additional hour or portion thereof that the	Three percent (3%) of the Fees for the month in which the initial Service Level Failure begins and three percent (3%) of such monthly Fees for the first additional hour or portion thereof that the corresponding Service Error remains un-

Support Request Classification	Service Level Metric (Required Response Time)	Service Level Metric (Required Resolution Time)	Service Level Credits (For Failure to Respond to any Support Request Within the Corresponding Response Time)	Service Level Credits (For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time)
	<p>generates email.</p> <p>The Response Time commences when Service Provider personnel respond either through a return phone call or placing a comment on Service Now. Autogenerated responses from a ticketing system are not considered responses for the purposes of calculating Response Time.</p>	<p>twenty-four (24) hours.</p>	<p>corresponding Service Error is not responded to within the required response time.</p>	<p>Resolved, which amount will thereafter double for each additional one-hour increment.</p>

Support Request Classification	Service Level Metric (Required Response Time)	Service Level Metric (Required Resolution Time)	Service Level Credits (For Failure to Respond to any Support Request Within the Corresponding Response Time)	Service Level Credits (For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time)
	Updates: every four (4) hours during support hours or time frame agreed upon by the State and Contractor.			
Medium Service Error	Three (3) hours in writing The Response Time commences when Service Provider personnel respond either through a return phone call, collaboration platform, or placing a comment on Service Now.	Ten (10) Business Days	N/A	N/A

Support Request Classification	Service Level Metric (Required Response Time)	Service Level Metric (Required Resolution Time)	Service Level Credits (For Failure to Respond to any Support Request Within the Corresponding Response Time)	Service Level Credits (For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time)
	Autogenerated responses from a ticketing system are not considered responses for the purposes of calculating Response Time.			
Low Service Error	Twenty-four (24) hours in writing The Response Time commences when Service Provider personnel respond either through a return phone call, collaboration platform, or	Ten (10) Business Days	N/A	N/A

Support Request Classification	Service Level Metric (Required Response Time)	Service Level Metric (Required Resolution Time)	Service Level Credits (For Failure to Respond to any Support Request Within the Corresponding Response Time)	Service Level Credits (For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time)
	<p>placing a comment on Service Now. Autogenerated responses from a ticketing system are not considered responses for the purposes of calculating Response Time.</p>			

3.7 Escalation. With respect to any Critical Service Error Support Request, until such Support Request is Resolved, Contractor will escalate that Support Request within sixty (60) minutes of the receipt of such Support Request by the appropriate Contractor support personnel, including, as applicable, the Contractor Project Manager and Contractor’s management or engineering personnel, as appropriate.

3.8 Support Service Level Credits. Failure to achieve any of the Support Service Level Requirements for Critical and High Service Errors will constitute a Service Level Failure for which Contractor will issue to the State the corresponding service credits set forth in **Section 3.6 (“Service Level Credits”)** in accordance with payment terms set forth in the Contract.

3.9 Corrective Action Plan. If two or more Critical Service Errors occur in any thirty (30) day period during (a) the Term or (b) any additional periods during

which Contractor does or is required to perform any Hosted Services, Contractor will promptly investigate the root causes of these Service Errors and provide to the State within five (5) Business Days of its receipt of notice of the second such Support Request an analysis of such root causes and a proposed written corrective action plan for the State's review, comment and approval, which, subject to and upon the State's written approval, shall be a part of, and by this reference is incorporated in, the Contract as the parties' corrective action plan (the "**Corrective Action Plan**"). The Corrective Action Plan must include, at a minimum: (a) Contractor's commitment to the State to devote the appropriate time, skilled personnel, systems support and equipment and other resources necessary to Resolve and prevent any further occurrences of the Service Errors giving rise to such Support Requests; (b) a strategy for developing any programming, software updates, fixes, patches, etc. necessary to remedy, and prevent any further occurrences of, such Service Errors; and (c) time frames for implementing the Corrective Action Plan. There will be no additional charge for Contractor's preparation or implementation of the Corrective Action Plan in the time frames and manner set forth therein.

4. Data Storage, Backup, Restoration and Disaster Recovery. Contractor must maintain or cause to be maintained backup redundancy and disaster avoidance and recovery procedures designed to safeguard State Data and the State's other Confidential Information, Contractor's Processing capability and the availability of the IT Environment Services and Software, in each case throughout the Term and at all times in connection with its actual or required performance of the Services hereunder. All backed up State Data shall be located in the continental United States. The force majeure provisions of this Contract do not limit Contractor's obligations under this section.

4.1 Data Storage. Contractor will provide sufficient storage capacity to meet the needs of the State at no additional cost.

4.2 Data Backup. Contractor will conduct, or cause to be conducted, daily back-ups of State Data and perform, or cause to be performed, other periodic offline back-ups of State Data on at least a weekly basis and store and retain such back-ups as specified in **Schedule A**. Contractor must, within five (5) Business Days of the State's request, provide the State, without charge and without any conditions or contingencies whatsoever (including but not limited to the payment of any fees due to Contractor), an extract of State Data in the format specified by the State.

4.3 Data Restoration. If the data restoration is required due to the actions or inactions of the Contractor or its subcontractors, Contractor will promptly notify the State and complete actions required to restore service to normal production

operation. If requested, Contractor will restore data from a backup upon written notice from the State. Contractor will restore the data within one (1) Business Day of the State's request. Contractor will provide data restorations at its sole cost and expense. Under no circumstances will data be overwritten.

4.4 Disaster Recovery. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will maintain and operate a backup and disaster recovery plan to achieve a Recovery Point Objective (RPO) of 4 hours, and a Recovery Time Objective (RTO) of 4 hours (the "**DR Plan**"), and implement such DR Plan in the event of any unplanned interruption of the Hosted Services. Contractor's current DR Plan, revision history, and any reports or summaries relating to past testing of or pursuant to the DR Plan are attached as **Schedule F**. Contractor will actively test, review and update the DR Plan on at least an annual basis using industry best practices as guidance. Contractor will provide the State with copies of all such updates to the Plan within fifteen (15) days of its adoption by Contractor. All updates to the DR Plan are subject to the requirements of this **Section 4**; and provide the State with copies of all reports resulting from any testing of or pursuant to the DR Plan promptly after Contractor's receipt or preparation. If Contractor fails to reinstate all material Hosted Services and Software within the periods of time set forth in the DR Plan, the State may, in addition to any other remedies available under this Contract, in its sole discretion, immediately terminate this Contract as a non-curable default.

SCHEDULE D – ATTACHMENT 1 – CONTACT LIST

Sandra Hunchak
Director, IT Delivery
300 – 10 Research Drive
Regina, SK S4S 7J7
Phone: (306) 787-7192
Email: Sandra.Hunchak@isc.ca

Tera Grieve
Senior Programmer Analyst
300 – 10 Research Drive
Regina, SK S4S 7J7
Phone: (306) 596-8372
Email: Tera.Grieve@isc.ca

SCHEDULE E – DATA SECURITY REQUIREMENTS

1. Definitions. For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this **Schedule** shall have the respective meanings given to them in the Contract.

“**Contractor Security Officer**” has the meaning set forth in **Section 2** of this Schedule.

“**FedRAMP**” means the Federal Risk and Authorization Management Program, which is a federally approved risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

“**FISMA**” means The Federal Information Security Modernization Act of 2014 (Pub.L. No. 113-283 (Dec. 18, 2014)).

“**Hosting Provider**” means any Permitted Subcontractor that is providing any or all of the Hosted Services under this Contract.

“**MOD**” means moderate.

“**NIST**” means the National Institute of Standards and Technology.

“**PCI**” means the Payment Card Industry.

“**PSP**” or “**PSPs**” means the State’s IT Policies, Standards and Procedures.

“**SSAE**” means Statement on Standards for Attestation Engagements.

“**Security Accreditation Process**” has the meaning set forth in **Section 6** of this Schedule

2. Security Officer. Contractor will appoint a Contractor employee to respond to the State’s inquiries regarding the security of the Hosted Services who has sufficient knowledge of the security of the Hosted Services and the authority to act on behalf of Contractor in matters pertaining thereto (“**Contractor Security Officer**”).

3. Contractor Responsibilities. Contractor is responsible for establishing and maintaining a data privacy and information security program, including physical, technical, administrative, and organizational safeguards, that is designed to:

- (a) ensure the security and confidentiality of the State Data;
- (b) protect against any anticipated threats or hazards to the security or integrity of the State Data;

- (c) protect against unauthorized disclosure, access to, or use of the State Data;
- (d) ensure the proper disposal of any State Data in Contractor's or its subcontractor's possession; and
- (e) ensure that all Contractor Personnel comply with the foregoing.

The State has established Information Technology (IT) PSPs to protect IT resources under the authority outlined in the overarching State 1305.00 Enterprise IT Policy. In no case will the safeguards of Contractor's data privacy and information security program be less stringent than the safeguards used by the State, and Contractor must at all times comply with all applicable public and non-public State IT policies and standards, of which the publicly available ones are at <https://www.michigan.gov/dtmb/policies/it-policies>.

This responsibility also extends to all service providers and subcontractors with access to State Data or an ability to impact the contracted solution. Contractor responsibilities are determined from the PSPs based on the services being provided to the State, the type of IT solution, and the applicable laws and regulations.

4. Acceptable Use Standard. To the extent that Contractor has access to the State's IT environment, Contractor must comply with the State's Acceptable Use Standard, see <https://www.michigan.gov/dtmb/-/media/Project/Websites/dtmb/Law-and-Policies/IT-Policy/13400013002-Acceptable-Use-of-Information-Technology-Standard.pdf>. All Contractor Personnel will be required, in writing, to agree to the State's Acceptable Use Standard before accessing State systems or Data. The State reserves the right to terminate Contractor's and/or subcontractor(s) or any Contractor Personnel's access to State systems if the State determines a violation has occurred.

5. Protection of State's Information. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will:

5.1 If Hosted Services are provided by a Hosting Provider, ensure each Hosting Provider maintains FedRAMP authorization for all Hosted Services environments throughout the Term, and in the event a Hosting Provider is unable to maintain FedRAMP authorization, the State, at its sole discretion, may either a) require the Contractor to move the Software and State Data to an alternative Hosting Provider selected and approved by the State at Contractor's sole cost and expense without any increase in Fees, or b) immediately terminate this Contract for cause.

5.2 for Hosted Services provided by the Contractor, maintain either a FedRAMP authorization or an annual contiguous SSAE 18 SOC 2 Type II audit based on State required NIST Special Publication 800-53 MOD Controls using identified controls and minimum values as established in applicable State PSPs. SOC 2 Type II audit reports on the Hosted Services must address all five trust principles of Security,

Availability, Confidentiality, Processing Integrity, and Privacy. The Contractor must provide its SSAE 18 SOC 2 Type II audit report to the State within thirty (30) days of the Contractor's receipt of such report.

5.3 For the Software provided by the Contractor, maintain either a FedRAMP authorization or an annual contiguous SSAE 18 SOC 2 Type II audit based on State required NIST Special Publication 800-53 MOD Controls using identified controls and minimum values as established in applicable State PSPs. SOC 2 Type II audit reports on the Software must address all five trust principles of Security, Availability, Confidentiality, Processing Integrity, and Privacy. Contractor must provide copies of such audit reports covering controls on its own organization as well as controls on its subcontractor organizations. Contractor must annually document how it meets each subcontractor organization's complementary user controls. The Contractor must provide its SSAE 18 SOC 2 Type II audit report to the State within thirty (30) days of the Contractor's receipt of such report. Any finding will be remediated within 6 months.

The Contractor will be required to have their SOC 2 Type II Report by **12/31/2024** date. Failure to complete and submit to the State the SOC 2 Type II Report by **12/31/2024** date will result in a \$1,000 credit per day.

5.4 ensure that the Software and State Data is securely stored, hosted, supported, administered, accessed, developed, and backed up in the continental United States and Canada, and the data center(s) in which State Data resides minimally meets Uptime Institute Tier 3 standards, or its equivalent; (<https://www.uptimeinstitute.com/>), or its equivalent;

5.5 maintain and enforce an information security program including safety and physical and technical security policies and procedures with respect to its Processing of the State Data that complies with the requirements of the State's data security policies as set forth in this Contract, and must, at a minimum, remain compliant with FISMA and NIST Special Publication 800-53 MOD Controls using identified controls and minimum values as established in applicable State PSPs;

5.6 Throughout the Term, Contractor must not provide Hardware or Services from the list of excluded parties in the System for Award Management (SAM) for entities excluded from receiving federal government awards for "covered telecommunications equipment or services.

5.7 provide technical and organizational safeguards against accidental, unlawful or unauthorized access to or use, destruction, loss, alteration, disclosure, encryption, transfer, commingling or processing of such information that ensure a level of security appropriate to the risks presented by the processing of State Data and the nature of such State Data, consistent with best industry practice and applicable

standards (including, but not limited to, compliance with FISMA, NIST, CMS, IRS, FBI, SSA, HIPAA, FERPA and PCI requirements as applicable);

5.8 take all reasonable measures to:

(a) secure and defend all locations, equipment, systems and other materials and facilities employed in connection with the Services against “malicious actors” and others who may seek, without authorization, to destroy, disrupt, damage, encrypt, modify, copy, access or otherwise use Hosted Services or the information found therein; and

(b) prevent (i) the State and its Authorized Users from having access to the data of other customers or such other customer’s users of the Services; (ii) State Data from being commingled with or contaminated by the data of other customers or their users of the Services; and (iii) unauthorized access to any of the State Data;

5.9 ensure that State Data is encrypted in transit and at rest using FIPS validated AES encryption modules and a key size of 128 bits or higher;

5.10 ensure the Hosted Services support Identity Federation/Single Sign-on (SSO) capabilities using Security Assertion Markup Language (SAML), Open Authentication (OAuth) or comparable State approved mechanisms;

5.11 ensure the Hosted Services implements NIST compliant multi-factor authentication for privileged/administrative and other identified access.

5.12 Contractor must permanently sanitize or destroy the State’s information, including State Data, from all media both digital and nondigital including backups using National Security Agency (“NSA”) and/or National Institute of Standards and Technology (“NIST”) (NIST Guide for Media Sanitization 800-88) data sanitization methods or as otherwise instructed by the State. Contractor must sanitize information system media, both digital and non-digital, prior to disposal, release out of its control, or release for reuse as specified above. Contractor must sign an Certificate of Destruction upon request.

6. Security Accreditation Process. Throughout the Term, Contractor will assist the State, at no additional cost, with its **Security Accreditation Process**, which includes the development, completion and on-going maintenance of a system security plan (SSP) using the State’s automated governance, risk and compliance (GRC) platform, which requires Contractor to submit evidence, upon request from the State, in order to validate Contractor’s security controls within two weeks of the State’s request. On an annual basis, or as otherwise required by the State such as for significant changes, re-assessment of the system’s controls will be required to receive and maintain authority to operate (ATO). All identified risks from the SSP will be remediated through a Plan of

Action and Milestones (POAM) process with remediation time frames and required evidence based on the risk level of the identified risk. For all findings associated with the Contractor's solution, at no additional cost, Contractor will be required to create or assist with the creation of State approved POAMs, perform related remediation activities, and provide evidence of compliance. The State will make any decisions on acceptable risk, Contractor may request risk acceptance, supported by compensating controls, however only the State may formally accept risk. Failure to comply with this section will be deemed a material breach of the Contract.

7. Unauthorized Access. Contractor may not access, and must not permit any access to, State systems, in whole or in part, whether through the Hosted Services or otherwise, without the State's express prior written authorization. Such authorization may be revoked by the State in writing at any time in its sole discretion. Any access to State systems must be solely in accordance with the Contract and this Schedule, and in no case exceed the scope of the State's authorization pursuant to this Section. All State-authorized connectivity or attempted connectivity to State systems shall be only through the State's security gateways and firewalls and in compliance with the State's security policies set forth in the Contract as the same may be supplemented or amended by the State and provided to Contractor from time to time.

8. Security Audits.

8.1 During the Term, Contractor will maintain complete and accurate records of its data protection practices, IT security controls, and the security logs relating to State Data, including but not limited to any backup, disaster recovery or other policies, practices or procedures relating to the State Data and any other information relevant to its compliance with this Contract.

8.2 Without limiting any other audit rights of the State, the State has the right to review Contractor's data privacy and information security program prior to the commencement of Services and from time to time during the term of this Contract. The State, at its own expense, is entitled to perform, or to have performed, an on-site audit of Contractor's data privacy and information security program. If the State chooses to perform an on-site audit, Contractor will, make all such records, appropriate personnel and relevant materials available during normal business hours for inspection and audit by the State or an independent data security expert that is reasonably acceptable to Contractor, provided that the State: (i) gives Contractor at least five (5) Business Days prior notice of any such audit; (ii) undertakes such audit no more than once per calendar year, except for good cause shown; and (iii) conducts or causes to be conducted such audit in a manner designed to minimize disruption of Contractor's normal business operations and that complies with the terms and conditions of all data confidentiality, ownership, privacy, security and restricted use provisions of the Contract. The State may, but is not obligated to,

perform such security audits, which shall, at the State's option and request, include penetration and security tests, of any and all Hosted Services and their housing facilities and operating environments.

8.3 During the Term, Contractor will, when requested by the State, provide a copy of Contractor's and Hosting Provider's FedRAMP System Security Plan(s) or SOC 2 Type 2 report(s) to the State within two weeks of the State's request. The System Security Plan and SSAE audit reports will be recognized as Contractor's Confidential Information.

8.4 With respect to State Data, Contractor must implement any required safeguards as identified by the State or by any audit of Contractor's data privacy and information security program.

8.5 The State reserves the right, at its sole election, to immediately terminate this Contract or a Statement of Work without limitation and without liability if the State determines that Contractor fails or has failed to meet its obligations under this **Section 8.**

9. Application Scanning. During the Term, Contractor must, at its sole cost and expense, scan all Contractor provided applications, and must analyze, remediate and validate all vulnerabilities identified by the scans as required by the State Secure Web Application and other applicable PSPs.

Contractor's application scanning and remediation must include each of the following types of scans and activities:

9.1 Dynamic Application Security Testing (DAST) – Scanning interactive application for vulnerabilities, analysis, remediation, and validation (may include Interactive Application Security Testing (IAST)).

(a) Contractor must either a) grant the State the right to dynamically scan a deployed version of the Software; or b) in lieu of the State performing the scan, Contractor must dynamically scan a deployed version of the Software using a State approved application scanning tool, and provide the State with a vulnerabilities assessment after Contractor has completed such scan. These scans and assessments i) must be completed and provided to the State quarterly (dates to be provided by the State) and for each major release; and ii) scans must be completed in a non-production environment with verifiable matching source code and supporting infrastructure configurations or the actual production environment.

9.2 Static Application Security Testing (SAST) - Scanning source code for vulnerabilities, analysis, remediation, and validation.

(a) For Contractor provided applications, Contractor, at its sole expense, must provide resources to complete static application source code scanning, including the analysis, remediation and validation of vulnerabilities identified by application source code scans. These scans must be completed for all source code initially, for all updated source code, and for all source code for each major release and Contractor must provide the State with a vulnerability assessment after Contractor has completed the required scans.

9.3 Software Composition Analysis (SCA) – Third Party and/or Open Source Scanning for vulnerabilities, analysis, remediation, and validation.

(a) For Software that includes third party and open source software, all included third party and open source software must be documented and the source supplier must be monitored by the Contractor for notification of identified vulnerabilities and remediation. SCA scans may be included as part of SAST and DAST scanning or employ the use of an SCA tool to meet the scanning requirements. These scans must be completed for all third party and open source software initially, for all updated third party and open source software, and for all third party and open source software in each major release and Contractor must provide the State with a vulnerability assessment after Contractor has completed the required scans if not provided as part of SAST and/or DAST reporting.

9.4 In addition, application scanning and remediation may include the following types of scans and activities if required by regulatory or industry requirements, data classification or otherwise identified by the State.

(a) If provided as part of the solution, all native mobile application software must meet these scanning requirements including any interaction with an application programming interface (API).

(b) Penetration Testing – Simulated attack on the application and infrastructure to identify security weaknesses.

10. Infrastructure Scanning.

10.1 For Hosted Services, Contractor must ensure the infrastructure and applications are scanned using an approved scanning tool (Qualys, Tenable, or other PCI Approved Vulnerability Scanning Tool) at least monthly and provide the scan's assessments to the State in a format that is specified by the State and used to track the remediation. Contractor will ensure the remediation of issues identified in the scan according to the remediation time requirements documented in the State's PSPs.

11. Nonexclusive Remedy for Security Breach.

11.1 Any failure of the Services to meet the requirements of this Schedule with respect to the security of any State Data or other Confidential Information of the State, including any related backup, disaster recovery or other policies, practices or procedures, is a material breach of the Contract for which the State, at its option, may terminate the Contract immediately upon written notice to Contractor without any notice or cure period, and Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination.

SCHEDULE E, Attachment 1 – PCI Compliance and CEPAS

1. PCI Compliance.

Contractors that process, transmit store or affect the security of credit/debit cardholder data, must adhere to the PCI Data Security Standard. The Contractor is responsible for the security of cardholder data in its possession. The data may only be used to assist the State or for other uses specifically authorized by law.

The Contractor must notify the State's Contract Administrator (within 48 hours of discovery) of any breaches in security where cardholder data has been compromised. In that event, the Contractor must provide full cooperation to the card associations (e.g. Visa, MasterCard, Discover, and American Express) and state acquirer representative(s), or a PCI approved third party, to conduct a thorough security review. The Contractor must provide, at the request of the State, the results of such third party security review. The review must validate compliance with the PCI Data Security Standard for protecting cardholder data. At the State's sole discretion, the State may perform its own security review, either by itself or through a PCI approved third party.

The Contractor is responsible for all costs incurred as the result of the breach. Costs may include, but are not limited to, fines/fees for non-compliance, card reissuance, credit monitoring, and any costs associated with a card association, PCI approved third party, or State initiated security review.

Without limiting Contractor's obligations of indemnification as further described in this Contract, Contractor must indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the breach.

The Contractor must dispose of cardholder data when it is no longer needed in compliance with PCI DSS policy. The Contractor must continue to treat cardholder data as confidential upon contract termination.

The Contractor must provide the State's Contract Administrator with an annual Attestation of Compliance (AOC) if or a Report on Compliance (ROC) showing the contractor is in compliance with the PCI Data Security Standard. The Contractor must notify the State's Contract Administrator of all failures to comply with the PCI Data Security Standard.

2. CEPAS Electronic Receipt Processing Standard.

All electronic commerce applications that allow for electronic receipt of credit or debit card and electronic check transactions must be processed via the State's Centralized Electronic Payment Authorization System (CEPAS). To minimize the risk to the State, full credit/debit card numbers, sensitive authentication data, and full bank account information must never be stored on state-owned IT resources.

SCHEDULE F – DISASTER RECOVERY PLAN

(Contractor's Disaster Recovery Plan is provided under separate cover)

SCHEDULE G – TRANSITION IN AND OUT

TRANSITION IN

The details regarding the Transition In phase are included in the broader proven RPM methodology for implementing RegSys UCC system for Michigan. Please refer to the Work Breakdown Structure in the Statement of Work section which describes how the Project Milestones will be achieved. As a brief recap, the purpose of the transition in phase is to:

- Monitor and control the project as agreed to in the project plan
- Perform a penetration test to ensure the environment is secured
- Complete the system, performance, and regression testing
- Complete UAT
- Complete training preparation
- Train Michigan staff

The exit criteria for the transition in phase is:

- Penetration test completed and results approved by Michigan
- UAT completed and system acceptance signed-off by Michigan
- System testing completed
- Performance testing completed
- Regression testing completed
- Training completed

TRANSITION OUT

The following describes the phases of a transition out plan and key milestones. The detailed plan to be followed for a transition out event would be finalized after identification of the third party the UCC system was moving to.

Key principles of the transition out plan include.

- ISC will fully cooperate with Michigan, and any subsequent contractor, in any activities related to turnover of responsibilities.
- ISC will continue to operate the registry at the scheduled rates
- The transition out plan details content migration and knowledge transfer activities
- ISC will return or destroy all Michigan data as appropriate by the close of the contract
- Upon completion, ISC will submit a confirmation report to be accepted by Michigan showing ISC has successfully completed

all outgoing transition activities.

ISC's Transition Out Framework has four phases.



Phase 1 – Initiating the Transition Framework

In the event of a Transition Triggering Event as per the agreement between the state and ISC, official notification from Michigan would be made to ISC.

The following steps and procedures would be followed within ISC:

1. A Transition Steering Committee would determine who will be required for the management of the transition, thus forming the ISC Transition Team.
2. The Transition Team will appoint a Transition Manager, who will manage the execution of the Transition Framework. The Transition Manager would possess the skills of an experienced project manager. The Transition Manager would be the leader of all activities performed under the Transition Framework and be the key point of contact for all parties involved.
3. The Transition Manager will lead the Transition Team to execute the Transition Framework.

The Transition Framework is prepared based on a key assumption that at the time of the Transition Triggering Event, the New Provider will be following similar steps, and will be appointing a transition manager and transition team of their own, with oversight by Michigan, to work with ISC. If the New Provider's transition team is not in place at the time of the Transition Triggering Event the execution of the Transition Framework could be delayed.

Phase 2 – Confirming the transition plan

Once the Transition Framework is initiated, execution of the Transition Framework would depend on the nature of the transition to take place, considering factors such as whether the services be provided by a new third-party provider or will the services be transitioned to the State of Michigan.

ISC acknowledges Michigan’s statement that the transition period could be up to 180 days with contracted payments to ISC for efforts made continuing during that time. That being said, a key assumption is that once the Transition Framework has been initiated, the members of the Transition Team will be dedicated to the execution of the Transition Framework, in the shortest time possible.

There will be dependencies between ISC and the New Provider to achieve a successful transition. As a result, a single, integrated transition plan (the “Transition Plan”) with a single owner is the best option to ensure all items on both sides are addressed on a timely and cooperative basis. The plan will be built as a joint activity between both transition teams. ‘Shared’ indicates a task shared between ISC, the New Provider and the State as described.

Phase 3 – Executing the transition plan

The finalized plan will utilize the project management best practices and methodology encompassing ISC, the New Provider and the State at the time of transition. The final plan will be dependent on circumstances as already described.

Phase 4 – Closeout

Once the final clean-up and disengagement steps are complete, ISC, the New Provider, and the State will enter into an agreement, as required, acknowledging that their respective work is complete, indicating acceptance of the Registry by the New Provider and the State, and addressing ISC’s further Registry responsibilities and liabilities, if any.

Transition Out Milestones

Milestones within the four phases would include the following. Milestones outline responsibilities and who’s involved.

Task	Description	ISC Participants	Responsibility
Establish ISC Transition Team	Confirm positions that make up ISC Transition Team and finalize personnel assignments.	Transition Steering Committee	ISC

Transition State Assessment	Determination of conditions and requirements affecting the transition. The items identified here will have a direct impact on the plan's tasks and durations. Confirm details regarding scenario that produced the Transition Triggering Event and the conditions that now exist (for example: length of time, specific date, other?) Identify possible external customer impacts?	Transition Steering Committee Transition Manager	Shared with Michigan
New Provider Assessment	Confirm details regarding the New Provider. For example: the underlying technological foundation, availability of key New Provider resources, etc.	Transition Manager, Transition Team	Shared with New Provider
Integrated Transition Plan	Finalize Transition Plan to be executed	Transition Team	Shared
Communication Plan	Determine requirements for internal and external Communication Management Plan, as appropriate	Transition Team	Shared
Data Migration	Identify data and prepare for data to be moved to replacement system	Transition Manager	ISC
Registry Access	Determine authorized requestors and individuals requiring access, setup of accounts for the New Provider (Registry accounts, network accounts), and appropriate accesses for the New Provider (documentation).	Transition Manager	Shared
Contracts	Develop and execute a detailed plan for the identification and transfer of any applicable contracts.	Transition Team	ISC
Transfer to new Software Platform	Itemize tasks, timing and resource assignments for the transfer for UCC services to the new software platform.	Transition Team	Shared
Document Transfer	Confirm tasks, timing and resource assignments for the	Transition Team	ISC

	movement of		
--	-------------	--	--

Knowledge and understanding of a registry transition out plan is not a theoretical event within ISC. As part of the 2013 process converting ISC from a government organization and assembling the organizational resources into a new publicly traded company the responsibility for, and operations of, the Vital Statistics registry left ISC in order to be retained by another part of government. As a result, this plan is founded upon the successful execution of a registry transfer.