STATE OF MICHIGAN PROCUREMENT

Department of Technology, Management, and Budget
525 W. Allegan St., Lansing, MI 48913

CONTRACT CHANGE NOTICE

Change Notice Number **1**
to
Contract Number **220000000887**

CONTRACTOR	Information Management Services, Inc.
	3901 Calverton Blvd. Suite 200
	Calverton, MD 20705
	Nicola Schussler
	(301) 680-9770
	schusslern@imsweb.com
	VS0192653

STATE	Program Manager	Vinod Narmat	DTMB
		(517) 290-9172	
		NarmatV@michigan.gov	
	Contract Administrator	Todd Huhn	DTMB
		(517) 335-0954	
		HuhnT@michigan.gov	

CONTRACT SUMMARY			
DESCRIPTION: SEER DMS instance for customization and ongoing support for Michigan Cancer Surveillance Program			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
07/01/2022	06/30/2025	3 – 1 year	06/30/2025
PAYMENT TERMS		DELIVERY TIMEFRAME	
Net 45		N/A	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
☐ P-card	☐ Payment Request (PRC)	☐ Other	☐ Yes ☒ No
MINIMUM DELIVERY REQUIREMENTS			
N/A			

DESCRIPTION OF CHANGE NOTICE				
OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☒	3 Years	☐		06/30/2028
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
$410,926.00	$211,102.00	$622,028.00		

DESCRIPTION: Effective at execution, this Contract is exercising all three option years and is increased by $211,102.00. The revised contract expiration date is 06/30/2028. Please note the State Program Manager has been changed to Vinod Narmat and the IMS Program Manager has been changed to Nicola Schussler. All other terms, conditions, specifications, and pricing remain the same. Per contractor and agency agreement, DTMB Central Procurement Services approval, and State Administrative Board approval on February 25, 2025.

STATEMENT OF WORK -
IT CHANGE NOTICE

Project Title: IMS Master Agreement Extension	**Period of Coverage:** 7/1/2025-6/30/2028
Requesting Department: Department of Health and Human Services	
Agency DHHS Project Manager: Jeff Duncan	**Phone**: (517) 335-8677
DTMB Project Manager: Vinod Narmat	**Phone**: (517) 290-9172

Brief description of services to be provided:

PROJECT OBJECTIVE:

The project objective is to exercise the 3 1-year option years available.

SCOPE OF WORK:

The Master Agreement is scheduled to end on June 30, 2025. This statement of work aims to exercise the 3 1-year option years extending the MA to 6/30/2028.

SPECIFIC DEPARTMENT STANDARDS:

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

PRICING

Please see Schedule B of the base Master Agreement for option year pricing.

PAYMENT SCHEDULE:

Payment will be made on a time and material basis. DTMB will pay the Vendor upon receipt of properly completed invoice(s) which shall be submitted to the billing address on the State issued purchase order not more often than monthly. DTMB Accounts Payable area will coordinate obtaining Agency and DTMB Project Manager approvals. All invoices should reflect actual work completed by payment date and must be approved by the Agency and DTMB Project Manager prior to payment. The invoices shall describe and document to the State's satisfaction a description of the work performed, the progress of the project, and fees. When expenses are invoiced, receipts will need to be provided along with a detailed breakdown of each type of expense.

The invoices shall document to the State's satisfaction.

- Project name
- Category of work performed (maintenance and operations, support and/or enhancements

- A description of the work performed,
- The timeframe when the work was performed,
- The purchase order number,
- An invoice number,
- The invoice date, and
- The amount to be paid.

Payment shall be considered timely if made by DTMB within forty-five (45) days after receipt of properly completed invoices.

Please note that the invoice shall be sent to dtmb-accounts-payable@michigan.gov.

EXPENSES:

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

PROJECT CONTACTS:

The designated DHHS Agency Project Manager is:

Jeff Duncan
Michigan Department of Health & Human Services
333 South Grand Ave.
Lansing, MI 48909
(517) 335-8677
Duncanj11@michigan.gov

The designated DTMB Project Manager is:

Vinod Narmat
Department of Technology, Management and Budget
Agency Services
235 South Grand Ave, 9th Floor
Lansing, MI 48933
(517) 290-9172
NarmatV@michigan.gov

The designated DTMB Project Manager is:

Todd Huhn
Department of Technology, Management and Budget
Office of Financial Services
320 South Walnut Street
Lansing, MI 48909
(517)335-0954
HuhnT@michigan.gov

STATE OF MICHIGAN PROCUREMENT

Department of Technology, Management, and Budget
525 W. Allegan St., Lansing, MI 48913

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. **220000000887**
between
THE STATE OF MICHIGAN
and

CONTRACTOR	Information Management Services, Inc.
	3901 Calverton Blvd. Suite 200
	Calverton, MD 20705
	Dave Annett
	(301) 680-9770
	AnnettD@imsweb.com
	VS0192653

STATE	Program Manager	Soopriya Razdan	DTMB
		(517) 219-2766	
		RazdanS@michigan.gov	
	Contract Administrator	Todd Huhn	DTMB
		(517) 335-0954	
		HuhnT@michigan.gov	

<table>
<tr><th colspan="4">CONTRACT SUMMARY</th></tr>
<tr><td colspan="4"><b>DESCRIPTION: SEER DMS instance for customization ongoing support for Michigan Cancer Surveillance Program</b></td></tr>
<tr><th>INITIAL EFFECTIVE DATE</th><th>INITIAL EXPIRATION DATE</th><th>INITIAL AVAILABLE OPTIONS</th><th>EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW</th></tr>
<tr><td>07/01/2022</td><td>06/30/2025</td><td>3 – 1 year</td><td>06/30/2025</td></tr>
<tr><th colspan="2">PAYMENT TERMS</th><th colspan="2">DELIVERY TIMEFRAME</th></tr>
<tr><td colspan="2">Net 45</td><td colspan="2">N/A</td></tr>
<tr><th colspan="3">ALTERNATE PAYMENT OPTIONS</th><th>EXTENDED PURCHASING</th></tr>
<tr><td colspan="3">☐ P-card ☐ Payment Request (PRC) ☐ Other</td><td>☐ Yes ☒ No</td></tr>
<tr><th colspan="4">MINIMUM DELIVERY REQUIREMENTS</th></tr>
<tr><td colspan="4"></td></tr>
<tr><th colspan="4">MISCELLANEOUS INFORMATION</th></tr>
<tr><td colspan="4">The purpose of this project is to support the state-wide Michigan Cancer Surveillance Program (MCSP) and the Metropolitan Detroit Cancer Surveillance System (MDCSS) in a single instance of SEER*DMS.</td></tr>
<tr><th colspan="2">ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION</th><td colspan="2"><b>$410,926.00</b></td></tr>
</table>

STATE OF MICHIGAN

IT PROFESSIONAL SERVICES

CONTRACT TERMS

This IT Professional Services Contract (the "**Contract**") is agreed to between the State of Michigan (the "**State**") and Information Management Services, Inc. ("**Contractor**"), a corporation. This Contract is effective on July 1, 2022, and unless terminated, expires on June 30, 2025.

This Contract may be renewed for up to three (3) additional one (1) year periods. Renewal must be by written notice from the State and will automatically extend the Term of this Contract.

The parties agree as follows:

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

"**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.

"**Confidential Information**" has the meaning set forth in **Section 21**.

"**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 **Section 5**.

"**Contract Change Notice**" has the meaning set forth in **Section 37**

"**Contractor**" has the meaning set forth in the preamble.

"**Contractor Personnel**" means all employees of Contractor or any Subcontractors involved in the performance of Services and creation of Work Product under this Contract.

"**Effective Date**" has the meaning set forth in the preamble.

"**Financial Audit Period**" has the meaning set forth in **Section 24**.

"**Key Personnel**" means any Contractor Personnel identified as key personnel in this Contract or the Statement of Work.

"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.

"**Services**" means any of the services Contractor, or any Subcontractor, is required to or otherwise does provide under this Contract, the Statement of Work or the Service Level Agreement.

"**Service Level Agreement**" means the service level agreement setting forth Contractor's support obligations for the Software, attached as **Schedule C** to this Contract.

"**Software**" means, collectively, the State's software applications and systems set forth in an appendix to the Statement of Work.

"**State**" has the meaning set forth in the preamble.

"**State Data**" has the meaning set forth in **Section 10.a.**

"**State Review Period**" has the meaning set forth in **Section 11**.

"**Statement of Work**" has the meaning set forth in **Section 2**.

"**Stop Work Order**" has the meaning set forth in **Section 13**.

"**Subcontractor**" has the meaning set forth in **Section 3.g**.

"**Transition Responsibilities**" has the meaning set forth in **Section 16**.

"**Unauthorized Removal**" has the meaning set forth in **Section 3.f.ii**.

"**Unauthorized Removal Credit**" has the meaning set forth in **Section 3.f.iii**.

"**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 developed in connection with this Contract whether or not embodied in this Contract.

2. **Statement of Work**. Contractor shall provide the Services and Work Product pursuant to the Statement of Work, attached as **Schedule A** to this Contract (the "**Statement of Work**"). The terms and conditions of this Contract will apply at all times to the Statement of Work. The State shall have the right to terminate the Statement of Work, in whole or in part, as set forth in **Sections 14 and 15** of this Contract.

3. **Performance of Services**.

   a. **Performance Warranty**. Contractor represents and warrants that its Services hereunder shall be performed by competent personnel and shall be of professional quality consistent with generally accepted industry standards for the performance of such services and shall comply in all respects with the requirements of this Contract and the specifications set forth in the Statement of Work and the Service Level Agreement. For any breach of this warranty, the State may, at its option, either terminate the Statement of Work immediately pursuant to the termination provision herein, or require Contractor to provide replacement personnel satisfactory to the State within thirty (30) calendar days of Contractor's receipt of notification from the State.

Whether or not the departing Contractor Personnel are to continue working while Contractor attempts to find replacement personnel is at the sole discretion of the State. If Contractor is notified within the first eight (8) hours of assignment that the person is unsatisfactory, Contractor will not charge the State for those hours; otherwise, the State shall pay for all actual hours worked prior to the State's notification of a replacement request to Contractor.

b. **Software Support**. Contractor shall provide support Services for the Software pursuant to the Service Level Agreement attached as **Schedule D** to this Contract.

c. **Accessibility Requirements**.

i. All Software and Work Product created or provided by Contractor under this Contract, including associated content and documentation, must conform to WCAG 2.0 Level AA. Contractor must provide a completed PAT for each such deliverable provided under the Contract. All "Not Applicable" or "N/A" responses to the specifications, if any, must be fully explained. A description of the evaluation methods used to support WCAG 2.0 Level AA conformance claims, including, if applicable, any third-party testing, must be provided. Throughout the Term of the Contract, at no additional costs to the State, Contractor must:

1. promptly respond to and resolve, in a manner acceptable to the State, any complaint the State receives regarding the accessibility of any Software or Work Product;

2. upon the State's written request, provide Software or Work Products in one or more alternative formats and within timeframes specified by the State; and

3. participate in the State of Michigan Digital Standards Review described below.

ii. <u>State of Michigan Digital Standards Review.</u> Prior to Software or Work Products being accepted, put into production, or as otherwise required by the State, the State may conduct a Digital Standards Review to assess their accessibility and compliance with WCAG 2.0 Level AA. Contractor must assist the State with each such review, including submitting documentation or other information regarding accessibility and compliance with WCAG 2.0 Level AA. Contractor must, at its sole cost and expense, remediate all issues resulting from such review in a manner and timeframe accepted in writing by the State, which may include providing a remediation status report and updated PAT to the State and a re-assessment of accessibility.

iii. Failure to comply with the requirements in this **Section 3** shall constitute a material breach of this Contract.

d. **Contractor Personnel**

i. 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.

ii. Prior to any Contractor Personnel performing any Services, Contractor will:

   1. ensure that such Contractor Personnel have the legal right to work in the United States;

   2. upon request, require such Contractor Personnel to execute written agreements, in form and substance acceptable to the State, that bind such Contractor Personnel to confidentiality provisions that are at least as protective of the State's information (including all Confidential Information) as those contained in this Contract; and

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. . The State, in its sole discretion, may also perform background checks on Contractor Personnel. 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.

iv. 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.

v. 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.

e. **Contractor's Key Personnel**

i. 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's Project Manager, 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.

ii. 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 14**.

iii. 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 fix 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 14**, Contractor will issue to the State the corresponding credits set forth below (each, an "**Unauthorized Removal Credit**"):

1. For the Unauthorized Removal of any Key Personnel designated in the Statement of Work, the credit amount will be $25,000.00 per individual if Contractor identifies a replacement approved by the State and assigns the replacement to shadow the Key Personnel who is leaving for a period of at least 30 calendar days before the Key Personnel's removal.

2. If Contractor fails to assign a replacement to shadow the removed Key Personnel for at least 30 calendar days, in addition to the $25,000.00 credit specified above, Contractor will credit the State $833.33 per calendar day for each day of the 30 calendar-day shadow period that the replacement Key Personnel does not shadow the removed Key Personnel, up to $25,000 maximum per individual. The total Unauthorized Removal Credits that may be assessed per Unauthorized Removal and failure to provide 30 calendar days of shadowing will not exceed $50,000.00 per individual.

iv. Contractor acknowledges and agrees that each of the Unauthorized Removal Credits assessed under **Subsection iii** 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.

f. **Subcontractors**. Contractor will not, without the prior written approval of the State, which consent may be given or withheld in the State's sole discretion, engage any third party to perform Services (including to create any Work Product). The State's approval of any such third party (each approved third party, a "**Subcontractor**") does not relieve Contractor of its representations, warranties or obligations under this Contract. Without limiting the foregoing, Contractor will:

i. be responsible and liable for the acts and omissions of each such Subcontractor (including such Subcontractor's employees who, to the extent providing Services or creating Work Product, shall be deemed Contractor Personnel) to the same extent as if such acts or omissions were by Contractor or its employees;

ii. name the State a third-party beneficiary under Contractor's contract with each Subcontractor with respect to the Services and Work Product;

iii. be responsible for all fees and expenses payable to, by or on behalf of each 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

iv. prior to the provision of Services or creation of Work Product by any Subcontractor, if requested by the State:

1. obtain from such Subcontractor confidentiality, work-for-hire and intellectual property rights assignment agreements, in form and substance acceptable by the State, giving the State rights consistent with those set forth in **Section 8** and, upon request, provide the State with a fully-executed copy of each such contract; and

2. with respect to all Subcontractor employees providing Services or Work Product, comply with its obligations under **subsection d** above.

4. **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:
Todd Huhn 320 S Walnut St. Lansing, MI 48909 huhnt@michigan.gov 517-335-0954	Dave Annett 3901 Calverton Blvd, Suite 200 Calverton, MD 20705 AnnettD@imsweb.com (301) 680-9770

5. **Contract Administrators.** The Contract Administrator for each party is the only person authorized to modify any terms and conditions of this Contract and are identified below:

State:	Contractor:
Todd Huhn 320 S Walnut St. Lansing, MI 48909 huhnt@michigan.gov 517-335-0954	Dave Annett 3901 Calverton Blvd, Suite 200 Calverton, MD 20705 AnnettD@imsweb.com (301) 680-9770

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

7. **Independent Contractor.** Contractor is an independent contractor and assumes all rights, obligations and liabilities set forth in this Contract. 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.

8. **Intellectual Property Rights**.

For avoidance of doubt, Contractor retains all right, title, and interest in the SEER*DMS software.

9. **Assignment.** Contractor may not assign this Contract to any other party without the prior written 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.

10. **Change of Control.** Contractor will notify the State, within 30 days of any public announcement or otherwise once legally permitted to do so. 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.

11. **Acceptance.** Unless otherwise provided in the Statement of Work, this Section shall control acceptance of all Services and Work Product, including deliverables. Services and Work Product, including deliverables are subject to inspection and testing by the State within 30 calendar days of the State's receipt of them ("**State Review Period**"). If the Services and Work Product, including 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 Services or Work Product, including deliverables are accepted, but noted deficiencies must be corrected; or (b) the Services or Work Product are rejected. If the State finds material deficiencies, it may: (i) reject the Services or Work Product, including deliverables without performing any further inspections; (ii) terminate a Statement of Work in accordance with **Section 14**, Termination for Cause.

Within 10 Business Days from the date of Contractor's receipt of notification of acceptance with deficiencies or rejection of any Services or Work Product, Contractor must cure, at no additional cost, the deficiency and deliver acceptable Services or Work Product to the State. If acceptance with deficiencies or rejection of the Services or Work Product impacts the content or delivery of other non-completed Services or Work Product, the parties 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.

If Contractor is unable or refuses to correct the deficiency within the time response standards set forth in this Contract, the State may cancel the Statement of Work in whole or in part. The State, or a third party identified by the State, may perform the Services and recover the difference between the cost to cure and the Contract price.

12. **Terms of Payment.** Invoices must conform to the requirements set forth in a Statement of Work. All undisputed amounts are payable within 45 days of the State's receipt. Contractor may only charge for Services and Work Product performed as specified in the Statement of Work. Invoices must include an itemized statement of all charges. The State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if Services and Work Product purchased under this Contract are for the State's exclusive use. Notwithstanding the foregoing, all prices 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.

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 or Work Product. 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.

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.

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. **Stop Work Order.** The State may suspend any or all activities under at a Statement of Work at any time. The State will provide Contractor a written stop work order detailing the suspension (a "**Stop Work Order**"). 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 Statement of Work. The State will not pay for Services or Work Product, Contractor's lost profits, or any additional compensation during a stop work period.

14. **Termination for Cause.** The State may terminate this Contract, in whole or in part (including individuals Statements of Work), if Contractor, as determined by the State: (a) endangers the value, integrity, or security of any State location, data, or personnel; (b) becomes insolvent, petitions for bankruptcy court proceedings, or has an involuntary bankruptcy proceeding filed against it by any creditor; (c) engages in any conduct that may expose the State to liability; (d) breaches any of its material duties or obligations under this Contract or the Statement of Work; or (e) fails to cure a breach within the time stated in a notice of breach. Any reference to specific breaches being material breaches within this Contract will not be construed to mean that other breaches are not material.

    If the State terminates this Contract under this Section, the State will issue a termination notice specifying whether Contractor must: (a) cease performance immediately, or (b) continue to perform for a specified period. If it is later determined that Contractor was not in breach of the 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 15**, Termination for Convenience.

    The State will only pay for amounts due to Contractor for Services and Work Product 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. The Contractor must pay all reasonable costs incurred by the State in terminating this Contract for cause, including administrative costs, attorneys' fees, court costs, and State Data transition costs.

15. **Termination for Convenience.** The State may immediately terminate this Contract, in whole or in part (including the Statement of Work), without penalty and for any reason, including but not limited to, appropriation or budget shortfalls. The termination notice will specify whether Contractor must: (a) cease performance of the Services immediately, or (b) continue to perform the Services in accordance with **Section 16**, Transition Responsibilities. 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.

16. **Transition Responsibilities.** Upon termination or expiration of this Contract for any reason, Contractor must, for a period of time specified by the State (not to exceed 90 calendar days), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the Services to continue without interruption or adverse effect, and to facilitate the orderly transfer of such Services to the State or its designees. Such transition assistance may include, but is not limited to: (a) continuing to perform the Services at the established Contract rates; (b) taking all reasonable and necessary measures to transition performance of the work, including all applicable Services, training, reports and other documentation, to the State or the State's designee; (c) taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, or return to the State all materials, data, property, and confidential information provided directly or indirectly to Contractor by any entity, agent, vendor, or employee of the State; (d) transferring title in and delivering to the State, at the State's discretion, all completed or partially completed Work Product prepared under this Contract as of the Contract termination date; and (e) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts (collectively, "**Transition Responsibilities**"). This Contract will automatically be extended through the end of the transition period.

17. **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 negligent or otherwise equally culpable 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).

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: (i) regular updates on proceeding status; (ii) participate in the defense of the proceeding; and (iii) employ its own counsel. Contractor will not, without the State's 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. To the extent that any State employee, official, or law may be involved or challenged, the State may, at its own expense, control the defense of that portion of the claim.

Any litigation activity on behalf of the State, or any of its subdivisions under this Section, 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.

18. **Infringement Remedies.** If, in either party's opinion, any of the Services or Work Product supplied by Contractor or its subcontractors, or its operation, use or reproduction, is likely to become the subject of a copyright, patent, trademark, or trade secret infringement claim, Contractor must, at its expense: (a) procure for the State the right to continue using the Services or Work Product, or if this option is not reasonably available to Contractor, (b) replace

or modify the same so that it becomes non-infringing; or (c) accept its return by the State with appropriate credits to the State against Contractor's charges and reimburse the State for any losses or costs incurred as a consequence of the State ceasing its use and returning it.

19. Disclaimer of Damages and Limitation of Liability.

a. 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.

b. 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.

20. State Data.

a. Ownership. The State's data ("**State Data**," which will be treated by Contractor as Confidential Information) includes any data collected, used, processed, stored, or generated as the result of the Services. 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. This Section survives the termination of this Contract.

b. 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, the Statement of Work, and applicable law; and (c) not use, sell, rent, transfer, distribute, 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. This Section survives the termination of this Contract.

c. Compromise of State 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, or integrity 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 twenty-four (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) perform or take any other actions required to comply with applicable law as a result of the occurrence; (d) 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; (e) pay for any costs associated with required notification and credit monitoring to affected individuals; and (f) 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. The parties agree that any damages relating to a breach of this **Section 20** are to be considered direct damages and not consequential damages. This Section survives termination or expiration of this Contract. Notwithstanding anything to the contrary set forth in this Section or any other provision of this Contract, the liability of Contractor for damages under this Section shall not exceed $5,000,000 per occurrence (the "Security Breach Indemnity Cap").

21. **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. The provisions of this Section survive the termination of this Contract.

a. 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 or is: (a) subject to disclosure under the Michigan Freedom of Information Act (FOIA) by the receiving party; (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 by, through, or on behalf of, the receiving party). For purposes of this Contract, in all cases and for all matters, State Data is deemed to be Confidential Information.

b. 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 a subcontractor is permissible where: (a) use of a subcontractor is authorized under this Contract; (b) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the subcontractor's responsibilities; and (c) Contractor obligates the subcontractor in a written contract to maintain the State's Confidential Information in confidence. At the State's request, any employee of Contractor or any subcontractor may be required to execute a separate agreement to be bound by the provisions of this Section.

c. 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 and each party will cooperate with the other party in seeking injunctive or other equitable relief against any such person.

d. 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 the Statement of Work corresponding to the breach or threatened breach.

e. Surrender of Confidential Information upon Termination. Upon termination or expiration of this Contract or a Statement of Work, in whole or in part, 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 sanitation 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 five (5) Business Days from the date of confirmation from the State. The retention period for off-site backups is one year. These provisions are applicable once the retention period expires.

22. **HIPAA Compliance**. Contractor agrees to comply, and ensure its Personnel comply, with the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder ("**HIPAA**") and Subtitle D of the Health Information Technology for Economic and Clinical Health Act, which is Title XIII of the American Recovery and Reinvestment Act of 2009 (Public Law 111-5) and any regulations promulgated thereunder with respect to the privacy and security of "protected health information" (as defined by HIPAA) accessed, created, transmitted, maintained or received by Contractor or its Personnel pursuant to, or in connection with, the performance of Contractor's or its Personnel's obligations under this Contract, including but not limited to entering into a Business Associate Agreement if required by law.

23. **Data Privacy and Information Security**. 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.

24. **Records Maintenance, Inspection, Examination, and Audit.** 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 the Contract through the term of the 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.

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 any 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 the Contract must be paid or refunded within 45 calendar days.

This Section applies to Contractor, any parent, affiliate, or subsidiary organization of Contractor, and any subcontractor that performs Services in connection with this Contract.

25. **Warranties and Representations.** Contractor represents and warrants to the State that: (a) It will perform all Services in a 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 the Statement of Work; (b) the Services and Work Product provided by Contractor will not infringe the patent, trademark, copyright, trade secret, or other proprietary rights of any third party; (c) it has the full right, power, and authority to enter into this Contract, to grant the rights granted under this Contract, and to perform its contractual obligations; (d) all information furnished and representations made in connection with the award of this Contract is true, accurate, and complete, and contains no false statements or omits any fact that would make the information misleading; and (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. A breach of this Section is considered a material breach of this Contract, which entitles the State to terminate this Contract under **Section 14**, Termination for Cause.

26. **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 subcontractor that performs Services in connection with this Contract.

27. **Compliance with Laws.** Contractor must comply with all applicable federal, state and local laws, rules and regulations.

28. **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, Vendor 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 (as defined in Executive Directive 2019-09), 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.

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

30. **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 Michigan Court of Claims. Contractor consents to venue in Ingham County, and waives any objections, such as lack of personal jurisdiction or *forum non conveniens*. Contractor must appoint agents in Michigan to receive service of process.

31. **Non-Exclusivity.** Nothing contained in this Contract is intended nor will be construed as creating any requirements contract with Contractor. This Contract does not restrict the State or its agencies from acquiring similar, equal, or like Services from other sources.

32. **Force Majeure.** Neither party will be in breach of this Contract because of any failure arising from any disaster or acts of God that are beyond their control and without their fault or negligence. Each party will use commercially reasonable efforts to resume performance. Contractor will not be relieved of a breach or delay caused by its subcontractors. If immediate performance is necessary to ensure public health and safety, the State may immediately contract with a third party.

33. **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 Project 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.

34. **Media Releases.** News releases (including promotional literature and commercial advertisements) pertaining to the Contract or project to which it relates must not be made without prior written State approval, and then only in accordance with the explicit written instructions of the State.

35. **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.

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

37. **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.

38. **Survival.** The provisions of this Contract that impose continuing obligations, including warranties and representations, termination, transition, insurance coverage, indemnification, and confidentiality, will survive the expiration or termination of this Contract.

39. **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 C	Insurance

Schedule D	Service Level Agreement
Schedule E	Data Security Requirements
Schedule F	Business Impact Analysis
Schedule G	Federal Provisions Addendum

40. **Entire Agreement.** This Contract, including the Schedules, 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, both written and oral, with respect to such subject matter. In the event of any conflict between the terms of this Contract and those of any Schedules, the following order of precedence governs: (a) first, this Contract; and (b) second, the Schedules. NO TERMS ON CONTRACTOR'S INVOICES, WEBSITE, BROWSE-WRAP, SHRINK-WRAP, CLICK-WRAP OR OTHER NON-NEGOTIATED TERMS AND CONDITIONS PROVIDED WITH ANY OF THE SERVICES, OR DOCUMENTATION HEREUNDER WILL CONSTITUTE A PART OR AMENDMENT OF THIS CONTRACT OR IS BINDING ON THE STATE FOR ANY PURPOSE. ALL SUCH OTHER TERMS AND CONDITIONS HAVE NO FORCE AND EFFECT AND ARE DEEMED REJECTED BY THE STATE, EVEN IF ACCESS TO OR USE OF SUCH SERVICE OR DOCUMENTATION REQUIRES AFFIRMATIVE ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

SCHEDULE A

Statement of Work
Implementation of SEER*DMS for the Michigan Cancer Surveillance Program and the Metropolitan Detroit Cancer Surveillance System

1. DEFINITIONS

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

TERM	DEFINITION
IMS	Information Management Services
DHHS	Michigan Department of Health and Human Services
DTMB	Michigan Department of Technology, Management and Budget
MCSP	Michigan Cancer Surveillance Program
CDC	Centers for Disease Control and Prevention
SEER	Surveillance, Epidemiology, and End Results
DMS	Data Management Software
HIPAA	Health Insurance Portability and Accountability Act, a 1996 Federal law that restricts access to individuals' private medical information
NCI	National Cancer Institute
NIH	National Institutes of Health
NPCR	National Program of Cancer Registries
SaaS	Software as a Service
SRP	Surveillance Research Program
MDCSS	Metropolitan Detroit Cancer Surveillance System
SEER*DMS	A DMS system created by IMS under contract with the NCI

2. BACKGROUND

The Division for Vital Records and Health Statistics (DVRHS) operates Michigan's Central Cancer Registry as required by Michigan law (Act 82 of 1984, MCL333.2619). A cancer registry assembles information about cancer. This information can be used to identify causes, trends, effective treatments, and areas where more research is required. The knowledge gained assists in improving public health.

Michigan's cancer registry is currently supported through a cooperative agreement with the Centers for Disease Control and Prevention (CDC) called the National Program of Cancer Registries (NPCR) which funds registries in 46 states. The National Cancer Institute (NCI), one of the National Institutes of Health (NIH), maintains a more comprehensive but smaller group of registries known as Surveillance, Epidemiology, and End Results (SEER). SEER registries capture more comprehensive case information that is used to support ongoing cancer research.

Using a Surveillance, Epidemiology, and End Results (SEER) data management system will allow the State of Michigan to benefit from innovative surveillance informatics developed by the national SEER program. Fifteen states and three regions already participate. (Metropolitan Detroit Cancer Surveillance System (MDCSS), based at Wayne State University, was a founding member of SEER and their operations and database are currently managed using SEER*DMS.)

3. PURPOSE

The purpose of this project is to support the state-wide Michigan Cancer Surveillance Program (MCSP) and the Metropolitan Detroit Cancer Surveillance System (MDCSS) in a single instance of SEER*DMS. This project includes the migration of state-wide data from MCSP into SEER*DMS MDCSS, the configuration of the combined system, and support of both organizations.

4. CONTRACT TERM

The contract overall term will be 3 years with 3, 1-year options.

5. SPECIFIC STANDARDS

IT Policies, Standards and Procedures (PSP)

Contractors are advised that the State has methods, policies, standards and procedures that have been developed over the years. All services and products provided must comply with all applicable State IT policies and standards.

Public IT Policies, Standards and Procedures (PSP):
https://www.michigan.gov/dtmb/0,5552,7-358-82547_56579_56755---,00.html

ADA Compliance

The State is required to comply with the Americans with Disabilities Act of 1990 (ADA), and has adopted a formal policy regarding accessibility requirements for websites and software applications. The State is requiring that Contractor's Solution, where relevant, to level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0. Contractor may consider, where relevant, the W3C's Guidance on Applying WCAG 2.0 to Non-Web Information and Communications Technologies (WCAG2ICT) for non-web software and content. http://www.michigan.gov/documents/dmb/1650.00_209567_7.pdf?20151026134621

IMS staff who develop software and Web-based resources for the Federal government must be familiar with Section 508 laws. IMS is working toward making SEER*DMS fully compliant. IMS will complete a Voluntary Product Accessibility Template for WCAG 2.0 (WCAG 2.0 VPAT) or other comparable document for the proposed Solution.

6. TYPE AND CAPACITY

Type of User	Access Type	Number of Users	Number of Concurrent Users
State Employees	Admin Access	6	6
SOM Contractors	Admin Access	3	1
Public	Admin Access	0	0

Contractor must be able to meet the expected number of concurrent Users.

7. ACCESS CONTROL AND AUDIT

The Contractor's solution must include documented plans to integrate with the State's IT Identity and Access Management (IAM) environment as described in the State of Michigan Digital Strategy (http://www.michigan.gov/dtmb/0,5552,7-150-56345_56351_69611-336646--,00.html), which consist of:

1. MILogin/Michigan Identity, Credential, and Access Management (MICAM)
    a. 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.
2. MILogin Identity Federation
    a. Allows federated single sign-on (SSO) for business partners, as well as citizen-based applications.
3. MILogin Multi Factor Authentication (MFA, based on system data classification requirements)
    a. Required for those applications where data classification is Confidential and Restricted as defined by the 1340.00 Michigan Information Technology Information Security standard (i.e. the proposed solution must comply with PHI, PCI, CJIS, IRS, and other standards).
4. MILogin Identity Proofing Services (based on system data classification requirements)
    a. 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.

8. DATA RETENTION

Data shall be retained in SEER*DMS for the entire term of this contract, plus six months, to allow a reasonable time afterward to migrate off this platform in the event the contract is not renewed.

9. SECURITY

Contractor must review the Data Security requirements set forth in Schedule D – Data Security Requirements. Contractor must note any exceptions to the security requirements by redlining Schedule D – Data Security Requirements.

10. END-USER 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.

Contractor must accommodate the latest browser versions 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 site traffic, measured using Sessions or Visitors (or)
- 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. For those browsers with 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.

11. INTEGRATION

There are no data integration services needed at this time, however the State may need integration services in the future. If needed, additional contractor staff required for integration services must be agreed to by the State at the rates set forth in Schedule B – Pricing Rate Card.

12. MIGRATION

Contractor to support the state-wide Michigan Cancer Surveillance Program (MCSP) and the Metropolitan Detroit Cancer Surveillance System (MDCSS) into a single instance of SEER*DMS. This project includes the migration of state-wide data from MCSP into SEER*DMS MDCSS, the configuration of the combined system, and support of both organizations. In support of this contract, IMS will perform the tasks detailed in the Milestones and Deliverables section.

13. TESTING SERVICES AND ACCEPTANCE

Contractor will undertake and coordinate testing activities described herein, prior to placing any system changes (i.e., enhancements and modifications) into production. The Contractor will also confirm that all functional objectives specified for these changes have been achieved. The Contractor will develop a test plan for any system change that details the activities; dependency risks, contingencies, assumptions, and resources required to fully test the change. The test plan will include creation of a project plan with test schedule, approach, and a statement of required and assigned resources with associated roles and responsibilities. The test plan will also include a go-no/go date for implementation that will be agreed upon with the State.

14. TRAINING SERVICES

If needed, Contractor will conduct webcasts to train registry staff during the beta testing period. Contractor will consult with State of Michigan staff to define the schedule of the webcasts.

15. SUPPORT AND OPERATIONS

Contractor must review the State's standard Service Level Agreement (SLA) attached as Schedule B. Contractor must note any exceptions to the SLA by redlining Schedule B – Service Level Agreement.

16. DOCUMENTATION

Contractor must provide 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.

The Contractor's user documentation must provide detailed information about all software features and functionality, enabling the State to resolve common questions and issues prior to initiating formal support requests.

17. TRANSITION SERVICES

Upon termination or expiration of the agreement, Contractor must, for a period of time specified by the State (not to exceed 90 calendar days), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the agreement 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: (a) continuing to perform the services at the established rates; (b) taking all reasonable and necessary measures to transition performance of the work, including all applicable services to the State or the State's designee; (c) taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, or return (in a format specified by the State) to the State all data stored in the solution; and (d) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts.

18. PRODUCTS AND SERVICES

a) Complete and validate the migration of MCSP data into SEER*DMS MDCSS; the State of Michigan will retain ownership of the migrated data.

   i) Define layouts of migration files

      (1) Collaborate with MCSP and MDCSS staff to identify the types of data to be migrated from the MCSP system into SEER*DMS. Consolidated and source abstracts, pathology reports, death certificates, and other data types will be reviewed and considered for migration.

      (2) Define the layout for the MCSP migration files based on the communications with MCSP and MDCSS.

   ii) Define migration logic

      (1) Collaborate with MCSP and MDCSS staff to define requirements related to the data migration. Requirements will be defined for combining data for patients who are in both registries; and to set new patient IDs for some data because a Patient ID in one registry would refer to a different person in the other registry. IMS will develop a detailed list of rules that need to be defined. IMS will facilitate the requirements analysis project, while registry staff will need to be actively involved.

   iii) Implement an import and workflow to load MCSP consolidated data.

   iv) Implement an import to load and link MCSP source record data.

   v) Deploy the combined database to the MDCSS beta server for review by MCSP, MDCSS, and IMS staff.

b) Convert the SEER*DMS MDCSS into a system that supports both MCSP and MDCSS

   i) Requirements Analysis

      (1) Governance of a Cancer/Tumor/Case (CTC) will be based on a registry flag. Rules defined by MDCSS and State leadership will define if all staff can work on any CTC, regardless of registry; or if tasks are assigned to staff based on their registry affiliation. The registry flag will also impact algorithms including workflow requirements, application of standard setter edits, etc.

   ii) Workflow

      (1) Activate SEER*DMS fields and options that support multiple registries in a single instance of SEER*DMS. Adjust workflow routing rules per requirements defined by MCSP and MDCSS. Implement registry-specific task assignment rules.

   iii) Data Imports

      (1) Add support for files submitted by hospitals and other organizations to MCSP. Add state specific NAACCR XML dictionaries. Implement new import algorithms for files that are submitted to MCSP but not MDCSS.

   iv) Module to Screen Records Submitted to MCSP and MDCSS

      (1) Review specifications provided by MCSP and MDCSS. Modify the screening algorithms to accommodate differences between state-wide and MDCSS reporting rules.

v) Matching Algorithms.

(1) Implement changes to patient and tumor level matching algorithms, per MCSP specifications.

vi) Auto-consolidation Algorithms.

(1) Activate auto-consolidation rules defined by the SEER*DMS auto-consolidation workgroup. Configure these rules, if required by MCSP specifications. Add new auto-consolidation rules for MCSP specific fields.

vii) System screens

(1) Add MCSP specific fields to screen layouts. Make adjustments, as necessary, to the record and Patient Set editors to accommodate MCSP specific data items or to remove data items not collected by MCSP.

viii) Edits

(1) Implement MCSP specific conditions for standard setter edits (NPCR call for data, NAACCR call for data, etc.) Implement edits for MCSP specific fields.

c) Provide Training

i) IMS will conduct webcasts to train registry staff during the beta-testing period. IMS staff will consult with registry staff to define the schedule for the webcasts.

d) Deliver Customized version of SEER*DMS for the use by the State of Michigan

i) Initial System Review

ii) Beta Test Release

iii) Production Release

e) Provide ongoing maintenance and user support for SEER*DMS

i) Manage system administration, database security, backups, and system maintenance

ii) Provide SEER*DMS application updates

iii) Provide technical support via telephone and email, Squish, and other electronic communications.

iv) Following the production release of SEER*DMS, annual ongoing maintenance costs will be required.

IT Environment Responsibilities

For client-to-site access, IMS's SSL-VPN with digital certificates or the Google Authenticator will be used to facilitate communications over the Internet to IMS for each registry staff member requiring access. A separate certificate or smart phone configuration will be provided to each registry staff member requiring access. Each registry staff member's full name and e-mail address will be required and maintained by IMS. The IMS VPN administrators will issue, maintain, and revoke these SSL-VPN credentials, as necessary. Only appropriate staff authorized by the registry director shall create, maintain, modify, and delete the SEER*DMS user accounts and roles unique to each registry staff member.

IMS VPN administrators will collaborate with the State's counterparts to maintain Gateway to Gateway VPN connections.

The VPN(s) will allow access to the IMS IP addresses associated with the registry's SEER*DMS services. The TLS/SSL protocol is necessary to access the Web based SEER*DMS system. The SFTP/SCP/SSH protocol is necessary for SEER*DMS auto-loading. The VPN(s) will not allow registry staff access to any IMS resources other than the IP address associated with registry's SEER*DMS services. Conversely, no IMS assets will be allowed any communications with registry IT assets.

For an IMS 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 IMS 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 IMS or subcontractor name(s), if applicable
Facilities	IMS Computer Centers Cyxtera datacenter 22860 International Drive Sterling, Virginia 20166 TierPoint datacenter 1401 Russell Street Baltimore, Maryland 21230
Infrastructure	Hardware has already been acquired for MDCSS
Platform	Enterprise level multi-platform
Application	SEER*DMS
Storage	FIPS 140-2 validated solutions for encrypting all data at rest. The all flash block tier is encrypted via software as part of the Pure Storage Purity operating system (NIST certificate #2467). The SATA based network attached tier is encrypted via software by the NetApp CryptoMod product (NIST certificate #3072). The all flash NAS tier also uses NetApp CryptoMod but adds self-encrypting SSDs (NIST certificate #2709). The backup appliances

	are encrypted via software using the Rubrik Cryptographic Library (NIST certificate #2658).
Backup	Enterprise level multi-platform software to handle routine backups. Center-wide data backups and virus detection routines are executed to ensure data integrity throughout the center. Offsite maintenance of the most recently completed set of backups
Development	

19. CONTRACTOR KEY PERSONNEL

Contractor Contract Administrator. Contractor must identify the individual appointed by it to (a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract.

Contractor
Name: Dave Annett **Address:** 3901 Calverton Blvd, Suite 200 Calverton, MD 20705 **Phone:** (301) 680-9770 **Email:** AnnettD@imsweb.com

Contractor Project Manager. Contractor must identify the Contractor Project Manager who will 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.

Contractor
Name: Linda Coyle **Address:** 3901 Calverton Blvd, Suite 200 Calverton, MD 20705 **Phone:** (301) 680-9770 work **Email:** coylel@imsweb.com

Contractor Service Manager. Contractor to provide name of individual to serve as primary contact with respect to the Services, who will have the authority to act on behalf of Contractor in matters pertaining to the receipt and processing of Support Requests and the Support Services.

Contractor
Name: Linda Coyle **Address:** 3901 Calverton Blvd, Suite 200 Calverton, MD 20705 **Phone:** (301) 680-9770 work **Email:** coylel@imsweb.com

Contractor Security Officer. Contractor to provide name of individual to respond to State inquiries regarding the security of the Contractor's systems. This person must have sufficient knowledge of the security of the Contractor Systems and the authority to act on behalf of Contractor in matters pertaining thereto.

Contractor
Name: Scott Depuy

Address: 3901 Calverton Blvd, Suite 200
Calverton, MD 20705
Phone: (301) 680-9770
Email: depuys@imsweb.com

20. CONTRACTOR PERSONNEL REQUIREMENTS
The Contractor must present certifications evidencing satisfactory Michigan State Police Background checks ICHAT and drug tests for all staff identified for assignment to this project.

In addition, proposed Contractor personnel will be required to complete and submit an RI-8 Fingerprint Card for the National Crime Information Center (NCIC) Finger Prints, if required by project. At this time, Finger Prints are not required but maybe at a later date if agreed to by the parties.

Contractor will pay for all costs associated with ensuring their staff meets all requirements.

Contractor must describe how they will meet the requirements set forth in this section.

21. 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: Todd Huhn **Phone: (517) 335-0954** **Email: HuhnT@michigan.gov**

State Project Manager. The State Project Manager will serve as the primary contact with regard to implementation Services who will have the authority to act on behalf of the State in approving Deliverables, and day to day activities.

DTMB Program Manager
Name: Soopriya Razdan **Phone: (517) 219-2766** **Email: razdans@michigan.gov**

Agency Business Owner. The Agency Business Owner will serve as the primary contact for the business area with regard to business advisement who will have the authority to act on behalf of the State in matters pertaining to the business Specifications.

Agency Program Manager
Name: Jeffrey Duncan **Phone: (517) 335-8677** **Email: DuncanJ11@michigan.gov**

<u>State Responsibilities for the Migration and Customization Period</u>

- Provide complete documentation for migration data within timelines defined in the project plan.

- Respond in a timely manner to requests for data and relevant documentation.
- Participate in requirements analysis via virtual meetings; and provide written information via the IMS project tracking system.
- Collaborate with the MDCSS and the Contractor to define the combined workflow and data governance rules.
- Fulfill responsibilities defined for the State in the Milestones and Deliverables section of this document within the specified timeline.

Ongoing State Responsibilities

- Review and understand local, state, and national data standards and reporting requirements.
- Implement procedures and processes to ensure that State staff are informed of changes to local, state, and national data standards and reporting requirements.
- Inform IMS of changes to local and state data standards in a timely manner.

22. MEETINGS

Contractor must participate in teleconferences, webcasts, or meetings, at no additional cost to the State as the State deems as necessary. The meetings shall not be considered begun or complete until initiated by the State. A meeting may be moved or cancelled by mutual consent in writing.

23. PROJECT CONTROL & REPORTS

The IMS Project Manager will monitor project implementation progress on a continual basis. IMS will provide a monthly status report during the migration and customization period. The status report will be provided to the State's Project Manager with the following information:

- 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 month, and the cumulative total to date for the project. Also, state whether the remaining hours are sufficient to complete 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.

Contractor shall give the State monthly electronic or other written reports and updates of:

A. Error Reports with description of error and time for resolution from Schedule C - Service Level Agreement.

B. Performance to response and time reports from Schedule D – Service Level Agreement

C. Annual Security Report

D. Progress report which must contain:

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

b. Risks: Indicate any risks, problems, or issues, which could delay the project or endanger its success.

c. Updates: New releases or bug fixes to be delivered by Contractor in the next month.

24. **PROJECT MANAGER**

The Contractor Project Manager will be responsible for defining and maintaining a project schedule for the migration and customization period. The project schedule must identify tasks, durations, forecasted dates and resources required by the Contractor to meet the timeframes 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.

Milestones/Deliverables for Implementation

The milestone schedule and associated deliverables are set forth below. IMS and the State shall complete the tasks per this defined schedule. IMS shall provide the following services to the Registry (individually a "Service" and collectively, the "Services"):

Milestone Event	Responsible Parties	Associated Milestone Deliverable(s)	Schedule
Project Planning	IMS, The State, and MDCSS	Project Kickoff Meeting	Contract Execution + 10 business days
Data Migration: Definition of Data Types	The State	Review current data management system to identify the types of data to be migrated into SEER*DMS. Meet with IMS and MDCSS to review. All categories of data must be identified including consolidated data, source abstract data, source pathology data, death certificate data, and any other source record data. Other ancillary data must also be identified, such as, physician and facility listings.	Execution + 15 business days
Data Migration: Field Definitions	The State	Provide list of standard NAACCR data items that are collected. Provide list of and documentation for non-standard fields maintained in consolidated data and source abstract data.	Execution + 15 business days
State to SEER*DMS Connectivity	The State	Collaborate with IMS and define VPN specifications to support access to SEER*DMS by state registry staff. Negotiate and execute an interconnection security agreement (ISA) with IMS.	Execution + 21 business days
Data Migration: File Layout	IMS	Define the layout for the MCSP migration files based on the communications with MCSP and MDCSS. Define NAACCR XML data dictionaries to be used for consolidated data and source	Execution + 21 calendar days

		abstract data. Non-standard fields will be defined in the user dictionary. Propose file layouts for other data types including pathology report and death certificate data.	
Data Migration: Consolidated & Source Abstract Data	The State	Extract consolidated data and source abstract data from current data management system and transfer to IMS via a secure transfer mechanism provided by IMS.	Execution + 30 calendar days Repeat at execution +90 and +120 calendar days.
Data Migration: Consolidated Data	IMS	Load first submission of consolidated data into the beta instance of SEER*DMS MDCSS.	Execution + 60 calendar days
Data Migration: Non-abstract Source Data	The State	Extract path report, death certificate, and other source data from current data management system and transfer to IMS via a secure transfer mechanism provided by IMS.	Execution + 60 calendar days Repeat at execution +90 and +120 calendar days.
Access to the SEER*DMS system	IMS and The State	Implement the VPN solution providing access to the SEER*DMS system via a secure connection. This will be accomplished either through a site-to-site VPN between the registry's network and the SEER*DMS server, or through a client-to-site VPN configured on an individual workstation Notify the State of Michigan Program Manager of any potential delays or issues with the secure connection.	Execution + 90 calendar days
VPN	IMS	Ensure that the VPN(s) allow SSL and SSH access to IMS's IP addresses associated with the Registry use and access to SEER*DMS. The SSL protocol is necessary to access the Web based SEER*DMS system. The SSH protocol is necessary for SEER*DMS auto-loading and other maintenance tasks. The VPN(s) shall not allow the Registry staff access to any of the IMS resources other than the IP address associated with the Registry's use and access of SEER*DMS. Conversely, no IMS IT assets, including computers, networks, and other information technology components, both physical and virtual, will be allowed	Production + 90 calendar days

		any communications with the Registry's IT assets	
Procedures for development, management, operation and security of connections	IMS	Establish procedures regarding the development, management, operation, and security of the connections between the Registry staff and the Registry Data maintained in SEER*DMS within the IMS Computer Center to ensure confidentiality and security of the Registry Data.	Execution + 90 calendar days
Document interconnection arrangements and security responsibilities	IMS	Document interconnection arrangements and security responsibilities for the Registry and IMS; specify business requirements for the connection.	Execution + 90 calendar days
Data Linkage: Abstracts	IMS	Implement a process to link source abstract data to consolidated data; load source abstract data into the beta instance of SEER*DMS MDCSS.	Execution + 90 calendar days
Data Linkage: Path Reports	IMS	Implement a process to link source pathology report data to consolidated data; load source pathology data into the beta instance of SEER*DMS MDCSS.	Execution + 120 calendar days
Data Linkage: Other Source Data	IMS	Implement a process to link death certificate and other source data to consolidated data; load source data into the beta instance of SEER*DMS MDCSS.	Execution + 120 calendar days
Migration Logic: Combining data from MCSP and MDCSS	IMS	Collaborate with MCSP and MDCSS staff to define requirements related to the data migration. Requirements will be defined for combining data for patients who are in both registries; and to set new patient IDs for some data because a Patient ID in one registry would refer to a different person in the other registry. IMS will develop a detailed list of rules that need to be defined. IMS will facilitate the requirements analysis project, while registry staff will need to be actively involved. Deploy the combined database to the MDCSS beta server for review by MCSP, MDCSS, and IMS staff.	Execution + 120 calendar days
Migration Logic: Data Governance Rules	IMS	Implement flags and scripts to support data governance rules. Governance of a CTC will be based on a registry flag. Rules defined by MDCSS and State leadership will define if all staff can work on any	Execution + 120 calendar days

		CTC, regardless of registry; or if tasks are assigned to staff based on their registry affiliation. The registry flag will also impact algorithms including workflow requirements, application of standard setter edits, etc.	
Implementation: Workflow	IMS	Activate SEER*DMS fields and options that support multiple registries in a single instance of SEER*DMS. Adjust workflow routing rules per requirements defined by MCSP and MDCSS. Implement registry-specific task assignment rules.	Execution + 150 calendar days
Implementation: Data Imports	IMS	Add support for files submitted by hospitals and other organizations to MCSP. Add state specific NAACCR XML dictionaries. Implement new import algorithms for files that are submitted to MCSP but not MDCSS	Execution + 150 calendar days
Implementation: Source record screening	IMS	Review specifications provided by MCSP and MDCSS. Modify the screening algorithms to accommodate differences between state-wide and MDCSS reporting rules.	Execution + 150 calendar days
Implementation: Source record matching	IMS	Implement changes to patient and tumor level matching algorithms, per MCSP specifications.	Execution + 150 calendar days
Implementation: Auto-consolidation	IMS	Activate auto-consolidation rules defined by the SEER*DMS auto-consolidation workgroup. Configure these rules, if required by MCSP specifications. Add new auto-consolidation rules for MCSP specific fields.	Execution + 150 calendar days
Implementation: Editing Screens	IMS	Add MCSP specific fields to screen layouts. Make adjustments, as necessary, to the record and Patient Set editors.	Execution + 150 calendar days
Implementation: Edits	IMS	Implement MCSP specific conditions for standard setter edits (NPCR call for data, NAACCR call for data, etc.) Implement edits for MCSP specific fields.	Execution + 150 calendar days
Authorize registry staff access	IMS	Authorize all appropriate registry staff with access to the Registry's Data in SEER*DMS. IMS shall protect the Registry's Data from unauthorized access	Execution+150 calendar days

Provide Training	IMS	IMS will conduct webcasts to train registry staff during the beta-testing period. IMS staff will consult with registry staff to define the schedule for the webcasts.	Execution + 150 calendar days
Deliver customized version of SEER*DMS	IMS	Final Beta Test Release	Execution + 150 calendar days
Data Migration: Final Transfer of all Consolidated & Source Data	The State	Extract the final cut of migration data and transfer to IMS. This package must include all consolidated and source data from the current data management system. The State will stop using their current data management system.	Execution + 170 calendar days
Deliver customized version of SEER*DMS	IMS	Production Release	Execution + 180 calendar days
Hosting and system operations support	IMS	Provide hosting and system operations support and maintenance for SEER*DMS. Manage system administration, database security, backups, and system maintenance. Provide SEER*DMS application updates. Provide technical support via telephone and email, Squish, and other electronic communications. Following the production release of SEER*DMS, annual ongoing maintenance costs will be required.	Ongoing

25. PRICING

Please see **Schedule B - Pricing** for a detailed description of all costs associated with maintaining and supporting the Solution, including all requested services set forth in the Contract..

If Contractor reduces its prices 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.

Travel and Expenses

The State does not pay for overtime or travel expenses.

26. ADDITONAL INFORMATION

The State reserves the right to purchase any additional services or products from the Contractor during the duration of the Contract.

SCHEDULE B

Pricing

Contract Year	Dates	Data Migration and Customization	Annual Hosting Fee	Maintenance and Technical Support Fee	Annual Security Assessment Fee	Total
Year 1	07/01/22-06/30/23	$212,000 *	$25,000	$30,000	$10,000	$277,000
Year 2	07/01/23-06/30/24		$25,500	$30,600	$10,200	$66,300
Year 3	07/01/24-06/30/25		$26,010	$31,212	$10,404	$67,626

*IMS will perform the migration and SEER*DMS customization for the State of Michigan under a time and material agreement.

Option Year Pricing

Contract Year	Dates		Annual Hosting Fee	Maintenance and Technical Support Fee	Annual Security Assessment Fee	Total
Option Year 1	07/01/25-06/30/26		$26,530	$31,836	$10,612	$68,979
Option Year 2	07/01/26-06/30/27		$27,061	$32,473	$10,824	$70,358
Option Year 3	07/01/27-06/30/28		$27,602	$33,122	$11,041	$71,765

- *Option Year pricing may change if the population of the State of Michigan exceeds 10,000,000.

Contractor may invoice monthly.

If Contractor reduces its prices for any of the 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.

Future Enhancements, Contractor Hourly Rates

The Contractor must utilize the following rates when providing the State with a fixed price proposal for all future enhancements. The fixed price proposal must include a breakdown by resource and rate per hour.

Rate Card:

Contractor Resource	Hourly Rate		
	Year 1	Year 2	Year 3
Project Manager (PM)	$204/hr.	$208.08/hr.	$212.24/hr.
Systems Analysts (SA):	$167/hr.	$170.34/hr.	$173.75/hr.
Programmer Analysts/Sr Programmer Analysts (PRG2)	$117/hr.	$119.34/hr.	$121.73/hr.
Senior Programmer/Programmer (PRG1)	$100/hr.	$102/hr.	$104.14/hr.

2% increase per hourly rate for each option year.

Schedule C

Insurance

Insurance Requirements. Contractor, at its sole expense, must maintain the insurance coverage identified below. All required insurance must: (a) protect the State from claims that may arise out of, are alleged to arise out of, or otherwise result from Contractor's or a subcontractor's performance; (b) be primary and non-contributing to any comparable liability insurance (including self-insurance) carried by the State; and (c) be provided by a company with an A.M. Best rating of "A-" or better, and a financial size of VII or better.

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.	
Workers' Compensation Insurance	
Minimal Limits: Coverage according to applicable laws governing work activities.	Waiver of subrogation, except where waiver is prohibited by law.
Employers Liability Insurance	
Minimal Limits: $500,000 Each Accident $500,000 Each Employee by Disease $500,000 Aggregate Disease.	
Privacy and Security Liability (Cyber Liability) Insurance	
Minimal 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.

If any of the required policies provide **claims-made** coverage, the Contractor must: (a) provide coverage with a retroactive date before the Effective Date of the Contract or the beginning of

Contract Activities; (b) maintain coverage and provide evidence of coverage for at least three (3) years after completion of the Contract Activities; and (c) if coverage is cancelled or not renewed, and not replaced with another claims-made policy form with a retroactive date prior to the Contract Effective Date, Contractor must purchase extended reporting coverage for a minimum of three (3) years after completion of work.

Contractor must: (a) provide insurance certificates to the Contract Administrator, containing the agreement or delivery order number, at Contract formation and within twenty (20) calendar days of the expiration date of the applicable policies; (b) require that subcontractors maintain the required insurance contained in this Section; (c) notify the Contract Administrator within five (5) business days if any insurance is cancelled; and (d) waive all rights against the State for damages covered by insurance. Failure to maintain the required insurance does not limit this waiver.

This Section 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

THE SOFTWARE IS CONTRACTOR HOSTED:

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 **Section** shall have the respective meanings given to them in the Contract.

"**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**.

"**Contractor Service Manager**" has the meaning set forth in **Section 1**.

"**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.**

"**Hosted Services**" has the meaning set forth in the Terms and Conditions.

"**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**" has the meaning set forth in the Contract.

"**Software Support Services**" has the meaning set forth in **Section 3**.

"**State Service Manager**" has the meaning set forth in **Section 1.1**.

"**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 provide 24-hour access to an online reporting system for non-emergency issues; and provide immediate response to urgent issues reported from 8:00 am to 8:00 pm M-F (excluding Federal holidays) E.S.T.

"**Support Request**" has the meaning set forth in **Section 3.5**.

"**Support Service Level Requirements**" has the meaning set forth in **Section 3.4**.

"**Term**" has the meaning set forth in the Contract.

1. Personnel

Contractor Personnel for the Hosted Services. Contractor will appoint a Contractor employee to serve as a primary contact with respect to the Services who will have the authority to act on behalf of Contractor in matters pertaining to the receipt and processing of Support Requests and the Software Support Services (the "**Contractor Service Manager**"). The Contractor Service Manager will be considered Key Personnel under the Contract.

1.1 State Service Manager for the Hosted Services. The State will appoint and, in its reasonable discretion, replace, a State employee to serve as the primary contact with respect to the Services who will have the authority to act on behalf of the State in matters pertaining to the Software Support Services, including the submission and processing of Support Requests (the "**State Service Manager**").

2. Service Availability and Service Availably 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 99.95% 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. All required scheduled downtime occurs at the request of the Registry. Security updates will occur on the first Saturday of every month from 7:30 AM to 9:00 AM EST unless otherwise set forth in a notification to the Registry.

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 95% 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 thirty (30) 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, if Contractor does not meet the availability requirements during the previous calendar month .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**
≥99.95%	None
<99.95% 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 technical support to registry managers and designees who will report problems and request changes. Provide 24-hour access to an online reporting system for non-emergency issues. All communication shall be triaged, logged, and responded to, in a timely manner.

(c) 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

(d) 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**, or, if determined to be an internet provider problem, open a trouble ticket with the internet provider; and

(iii) Notifying the State 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 notifies the State prior to modifying or upgrading Hosting Services and Software, including Maintenance Releases and New Versions of Software; and

(b) all such services and repairs as are required to maintain the Hosting Services and Software or are ancillary, necessary or otherwise related to the State's or its Authorized Users' access to or use of the Hosting Services and Software, so that the Hosting 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 3.4** ("**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**"). The State Service Manager will notify Contractor of Support Requests by email, telephone or such other means as the parties may hereafter agree to in writing. All communication shall be sorted, triaged, logged and responded to, in a timely manner System failures or deficiencies that prevent timely completion of the State submission to national data standards will be considered a Critical Service Error.

Support Request Classification	**Description:** **Any Service Error Comprising or Causing any of the Following Events or Effects**
Critical Service Error	• Issue affecting entire system or single critical production function; • System down or operating in materially degraded state; • Data integrity at risk; • Widespread access interruptions.

High Service Error	- Primary component failure that materially impairs its performance; or - Data entry or access is materially impaired on a limited basis.
Medium Service Error	- IT Environment Services and Software is operating with minor issues that can be addressed with an acceptable (as determined by the State) temporary work around.
Low Service Error	- 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 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	One (1) hour	Three (3) hours	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	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

			corresponding Service Error is not responded to within the required response time.	the corresponding Service Error remains un-Resolved, which amount will thereafter double for each additional one-hour increment.
High Service Error	One (1) hour	Four (4) hours	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 corresponding Service Error is not responded to within the required response time.	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-Resolved, which amount will thereafter double for each additional one-hour increment.
Medium Service Error	Three (3) hours	Two (2) Business Days	N/A	N/A
Low Service Error	Three (3) hours	Five (5) Business Days	N/A	N/A

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 Service 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. Support Service Level Credits will be applied to the next annual invoice and will not exceed Twenty-Five (25%) Percent of the invoice total.

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 Hosting 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. 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**.**

4.2 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 back-ups of State Data on at least a weekly basis and store and retain such back-ups as specified in **Schedule A**.

4.3 Data Restoration. Contractor will restore data from a backup upon written notice from the State. Contractor will restore the data within five (5) Business Days of the State's request. Contractor will provide up to one (1) data restoration per year at its sole cost and expense, for any data loss that is the result of the State's actions. The State will reimburse Contractor for any additional data restorations for any data loss that is a result of the State's actions at the rates specified in **Schedule B** – Pricing. If the data restoration is required due to the actions or inactions of the Contractor or its subcontractors, the data restoration will not count against the quarterly data restoration or require the State to reimburse Contractor for the restoration.

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 as set forth in Schedule F Business Impact Analysis.

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.

"**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 Representatives 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/0,5552,7-358-82547_56579_56755---,00.html.

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 Policy. To the extent that Contractor has access to the State's IT environment, Contractor must comply with the State's Acceptable Use Policy, 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 Policy before accessing State systems. 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 pursuant to **Section 15.1** of the Contract;

5.2 for Hosted Services provided by the Contractor, maintain either a FedRAMP authorization or an annual 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.

5.3 ensure that the Software and State Data is securely hosted, supported, administered, accessed, and backed up in a data center(s) that resides in the continental United States, and minimally meets Uptime Institute Tier 3 standards (www.uptimeinstitute.com), or its equivalent;

5.4 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;

5.5 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);

5.6 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;

5.7 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;

5.8 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;

5.9 ensure the Hosted Services implements NIST compliant multi-factor authentication for privileged/administrative and other identified access.

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 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 and perform related remediation activities. 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 shall 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 ten (10) 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 or 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 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 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 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 programing 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 F – Business Impact Analysis

NIH NATIONAL CANCER INSTITUTE

Business Impact Analysis for

Surveillance, Epidemiology, and End Results Data Management System (SEER*DMS)

NCI

Security Categorization: Moderate

Version 1.1

May 24, 2022

Prepared by
Scott Depuy

FOR OFFICIAL USE ONLY

Document Revision History

This SEER*DMS Business Impact Analysis (BIA) is a living document that is changed as required to reflect system, operational, or organizational changes. Modifications made to this document are recorded in the version history matrix below.

At a minimum, this document will be reviewed and assessed annually. Reviews made as part of the assessment process shall also be recorded below.

This document history shall be maintained throughout the life of the document and the associated system.

Date	Description	Version	Author
10/16/2020	Document Publication	1.0	Scott Depuy – IMS, Inc.
5/24/2022	Update registry lists and inventories	1.1	Scott Depuy – IMS, Inc.

Business Impact Analysis Approval Signatures

I have reviewed the SEER*DMS Business Impact Analysis and accept the analysis and findings within.

DocuSigned by:
Marina Matatova May 31, 2022
4EC8E84AB1124AE...
Marina Matatova
NCI System Owner

DocuSigned by:
Karen Friend June 6, 2022
6097625ADF7540D...
Karen Friend
NCI Alt Information System Security Officer

Table of Contents

1 Overview

This Business Impact Analysis (BIA) is developed as part of the contingency planning process for SEER*DMS.

1.1 Purpose

The purpose of this BIA is to identify and prioritize SEER*DMS components as each relates to NIH's missions and goals. Using this information, the BIA categorizes and shows the overall business impact to NIH when components or the entire SEER*DMS is lost due to outage or a major contingency event.

1.2 NIH Mission and Goals[1]

NIH's mission is to seek fundamental knowledge about the nature and behavior of living systems and the application of that knowledge to enhance health, lengthen life, and reduce illness and disability.

The goals of the agency are:

- to foster fundamental creative discoveries, innovative research strategies, and their applications as a basis for ultimately protecting and improving health;
- to develop, maintain, and renew scientific human and physical resources that will ensure the Nation's capability to prevent disease;
- to expand the knowledge base in medical and associated sciences in order to enhance the Nation's economic well-being and ensure a continued high return on the public investment in research; and
- to exemplify and promote the highest level of scientific integrity, public accountability, and social responsibility in the conduct of science.

In realizing these goals, the NIH provides leadership and direction to programs designed to improve the health of the Nation by conducting and supporting research:

- in the causes, diagnosis, prevention, and cure of human diseases;
- in the processes of human growth and development;
- in the biological effects of environmental contaminants;
- in the understanding of mental, addictive and physical disorders; and
- in directing programs for the collection, dissemination, and exchange of information in medicine and health, including the development and support of medical libraries and the training of medical librarians and other health information specialists.

[1] National Institutes of Health. (2015, April 9). About NIH. Retrieved from What We Do: Mission and Goals: https://www.nih.gov/about-nih/what-we-do/mission-goals.

1.3 BIA Steps

The three steps used to conduct this BIA are as follows:

- Determine SEER*DMS component and recovery criticality:
  - Determine the SEER*DMS functions supported by the system
  - Identify outage impacts & estimate the maximum downtime NIH can tolerate and still maintain its mission and goals

- Identify resource requirements
  - Identify and evaluate resources required (facilities, personnel, equipment, software, data files, and system components) to resume SEER*DMS operations as quickly as possible

- Identify recovery priorities for system resources
  - Based upon the results from the previous activities, identify the system resources that are linked to critical NIH missions and goals
  - Establish priority levels for sequencing recovery activities and resources

2 System Identification

2.1 System Name/Title

Unique Identifier (UUID)	Information System Name	Information System Abbreviation
SEER*DMS	SEER Data Management System	SEER*DMS

2.1.1 Responsible NIH Organization

IC Name	Shared Accountability Partner(s)
NCI	NCI

2.2 System Type and Purpose

SEER*DMS is a Minor Application.

The SEER Data Management System (SEER*DMS) is a centrally designed data management system for population-based cancer registries. SEER*DMS supports the core data processing requirements of a cancer registry – importing, linking, consolidating, and reporting cancer surveillance data. It is utilized by central cancer registries to process and submit cancer data to the SEER Program and other standard setters. The Surveillance, Epidemiology, and End Results (SEER) Program funded the development of SEER*DMS. The centralized system design and development improves data quality and consistency, increases efficiency, and reduces registry operation costs. All aspects of the system can be customized to meet the needs of individual registries.

The SEER Program funds and oversees the continued development and maintenance of the SEER*DMS application. In accordance with data ownership and stewardship requirements, each registry has their own instance of the SEER*DMS application and database. Each registry's instance is hosted by IMS in a SEER*DMS "application island", a construct that logically limits access to authorized users.

Access to each SEER*DMS island is limited to the registry and organizations approved by the registry. Each island has a defined boundary to enhance data security. The cancer registry data housed in SEER*DMS include PII and PHI related to all cancer cases diagnosed in the registry's geographic area. These data are secured within the system and only accessed by registry personnel via a VPN (secure link) to the island. This allows the data to be hosted and secured in the IMS infrastructure but still be managed by the registry.

2.3 System Operational Status

The system is currently in the Operational phase of the system development life cycle.

2.4 Security Categorization

SEER*DMS was evaluated against FIPS 199 and NIST SP 800-60 Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*. The following FIPS 199 security impact ratings are outlined in the *SEER*DMS Security Categorization* (see approved FIPS-199).

Security Objective	Low, Moderate or High
Confidentiality	Moderate
Integrity	Moderate
Availability	Moderate
Overall	**Moderate**

2.5 System Owner

Name	Marina Matatova
Title	Informatics Program Manager, Surveillance Informatics Branch
IC Name	NCI
Address	9609 Medical Center Drive, Rockville, Maryland 20850
Telephone	240.276.6269
Email	marina.matatova@nih.gov
Responsibility	Technical Project Management; Software and System Development Governance

2.6 Information System Security Office (ISSO)

Name	Karen Friend
Title	NCI Information System Security Officer
IC Name	NCI
Address	9609 Medical Center Drive, Rockville, Maryland 20850
Telephone	240.276.5055
Email	karen.friend@nih.gov
Responsibility	Information System Security Officer

2.7 IC Chief Information Officer

Name	Jeff Shilling
Title	NCI Chief Information Officer
IC Name	NCI
Address	9609 Medical Center Drive, Rockville, Maryland 20850
Telephone	240.276.5549
Email	jeffrey.shilling@nih.gov
Responsibility	Chief Information Officer

3 BIA Data Collection

*3.1 Step 1: Determine SEER*DMS Components and Recovery Criticality*

3.1.1 SEER*DMS Components and Descriptions

Component	Description
IMS firewall, VPN, and IPS	One high availability pair in each co-location facility
Production: Postgres server	CentOS 7 server for each of: Alaska, Arkansas, Cherokee Nation, Florida, Idaho, Illinois, Iowa, Kentucky, Massachusetts, New Mexico, Connecticut, Detroit, Georgia, Hawaii, Louisiana, Minnesota, New Jersey, New York, Ohio, Seattle, Tennessee, Texas, Utah, and NCCR
Production: application/web server	CentOS 7 server for each of: Alaska, Arkansas, Cherokee Nation, Florida, Idaho, Illinois, Iowa, Kentucky, Massachusetts, New Mexico, Connecticut, Detroit, Georgia, Hawaii, Louisiana, Minnesota, New Jersey, New York, Ohio, Seattle, Tennessee, Texas, Utah, and NCCR
Test, alpha, and beta tiers: Postgres server	CentOS 7 server for each of: Alaska, Arkansas, Cherokee Nation, Florida, Idaho, Illinois, Iowa, Kentucky, Massachusetts, New Mexico, Connecticut, Detroit, Georgia, Hawaii, Louisiana, Minnesota, New Jersey, New York, Ohio, Seattle, Tennessee, Texas, Utah, and NCCR
Test, alpha, and beta tiers: application/web server	CentOS 7 server for each of: Alaska, Arkansas, Cherokee Nation, Florida, Idaho, Illinois, Iowa, Kentucky, Massachusetts, New Mexico, Connecticut, Detroit, Georgia, Hawaii, Louisiana, Minnesota, New Jersey, New York, Ohio, Seattle, Tennessee, Texas, Utah, and NCCR

3.1.2 Outage Impacts and Estimated Downtime

<u>Outage Impacts</u>

The following impact categories represent important areas for consideration in the event of an outage:

Impact Category	Impact Values		
	Severe *(Systems in this category should consider fault-tolerant architecture and design)*	**Moderate** *(Systems in this category should consider alternate site processing options, or have tested rapid recovery processes)*	**Minimal** *(Systems in this category can tolerate prolonged disruptions, and do not require fault-tolerant or rapid recovery solutions)*
Cost	$1M+	$250K-$1M	<$250K

Impact Category	**Impact Values**		
	Severe *(Systems in this category should consider fault-tolerant architecture and design)*	**Moderate** *(Systems in this category should consider alternate site processing options, or have tested rapid recovery processes)*	**Minimal** *(Systems in this category can tolerate prolonged disruptions, and do not require fault-tolerant or rapid recovery solutions)*
Service Delivery	Disruption has a severe to catastrophic negative effect on the ability for NCI to perform its mission.	Disruption has a limited to severe negative effect on the ability for NCI to perform its mission.	Disruption has no, or only limited impact on NCI's ability to perform its mission.
Image/Credibility	Disruption has a severe to catastrophic negative effect on NCI's reputation or credibility.	Disruption has a noticeable to severe negative effect on NCI's reputation or credibility.	Disruption has no negative impact NCI's reputation or credibility.
Health & Safety	Disruption has a severe to catastrophic (unacceptable) negative effect on the health and safety of patients, staff, animals, or other NCI stakeholders.	Disruption has minimal to severe negative effect on the health and safety of patients, staff, animals, or other NCI stakeholders.	Disruption has no health or safety impacts.
Regulatory	Disruption has an unacceptable negative effect on NCI's regulatory mission.	Disruption has a limited negative effect on NCI's regulatory mission.	Disruption has no negative impact on NCI's regulatory mission.

The table below summarizes the impact for each SEER*DMS component on NIH's missions and goals if the component were unavailable:

SEER*DMS Component	**Impact Category**					
	Cost	**Service Delivery**	**Image/ Credibility**	**Health & Safety**	**Regulatory**	**Overall Impact**
IMS firewall, VPN, and IPS	Moderate	Moderate	Moderate	N/A-Minimal	Moderate	Moderate
Production: Postgres server	Moderate	Moderate	Moderate	N/A-Minimal	N/A-Minimal	Moderate
Production: application/web server	Moderate	Moderate	Moderate	N/A-Minimal	N/A-Minimal	Moderate
Test, alpha, and beta tiers: Postgres server	N/A-Minimal	N/A-Minimal	N/A-Minimal	N/A-Minimal	N/A-Minimal	N/A-Minimal
Test, alpha, and beta tiers: application/web server	N/A-Minimal	N/A-Minimal	N/A-Minimal	N/A-Minimal	N/A-Minimal	N/A-Minimal

Estimated Downtime

The estimated downtime factors are as follows:

- **Maximum Tolerable Downtime (MTD):** The MTD represents the total amount of time leaders/managers are willing to accept for a SEER*DMS component outage or disruption and includes all impact considerations.

- **Recovery Time Objective (RTO):** RTO defines the maximum amount of time that a SEER*DMS component can remain unavailable before there is an unacceptable impact on other NIH resources and the MTD.[2]

- **Recovery Point Objective (RPO):** The RPO represents the point in time, prior to a disruption or system outage, to which SEER*DMS component data must be recovered (given the most recent backup copy of the data) after an outage.

[2] Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.

The drivers for the MTD, RTO, and RPOs are as follows:

- Continuance of the SEER Program's mission in providing information on cancer statistics in an effort to reduce the cancer burden among the U.S. population. SEER provides national leadership in the science of cancer surveillance as well as analytical tools and methodological expertise in collecting, analyzing, interpreting, and disseminating reliable population-based cancer statistics.
- The data collected and managed via SEER*DMS are also vital to the mission of the NCI's Surveillance Research Program and Division of Cancer Control and Population Sciences.
- SEER also supports research activities such as: 1) patterns of care/quality of care studies, 2) a residual tissue repository program, and 3) SEER linked databases.

The table below identifies the MTD, RTO, and RPO (as applicable) for the SEER*DMS components:

SEER*DMS Component	MTD	RTO	RPO
IMS firewall, VPN, and IPS	48 hours	24 hours	12 hours
Production: Postgres server	48 hours	24 hours	1 hour
Production: application/web server	48 hours	24 hours	1 hour
Test, alpha, and beta tiers: Postgres server	2 weeks	10 days	N/A
Test, alpha, and beta tiers: application/web server	2 weeks	10 days	N/A

Alternative Means of Recovering SEER*DMS Operations

Both IMS co-location facilities are equally capable and conduct primary operations for some of the current 18 registies. Each datacenter also hosts a backup copy of the data for some of the registries. For each registry, data is continually being copied from the primary to the backup co-location facility such that no more than one hour of work will be lost in a catostropic event.

In the event that a co-location facility is "lost", each registries' application island and hosts will be provisioned in the surviving co-location facility and the data will be restored from backup. IMS performs annual drills of this disaster recovery operation, quarterly database recovery drills for Postgres, and monthly content restore drills for material stored in the filesystem.

3.2 Step 2: Identify Resource Requirements

3.2.1 Physical/Host Locations

Common Name/Reference	Physical Address
Baltimore co-location facility (TierPoint)	1401 Russell Street, Baltimore, MD 21230
Sterling co-location facility (Cyxtera)	22860 International Drive, Sterling, VA 20166

3.2.2 Physical Resources

TYPE	NAME	DNS NAME	IP ADDRESS	GUEST OS	SEER*DMS COMPONENT	ASSET TAG	LOCATION (Common Name)
Physical	BTPHosting01	N/A - Internal	172.22.16.49	ESXI	Hypervisor	1244	Baltimore
Physical	BTPHosting02	N/A - Internal	172.22.16.50	ESXI	Hypervisor	1242	Baltimore
Physical	BTPHosting03	N/A - Internal	172.22.16.131	ESXI	Hypervisor	1240	Baltimore
Physical	BTPHosting04	N/A - Internal	172.22.16.36	ESXI	Hypervisor	1238	Baltimore
Physical	BTPHosting05	N/A - Internal	172.22.16.51	ESXI	Hypervisor	010847	Baltimore
Physical	STHosting01	N/A - Internal	172.22.64.68	ESXI	Hypervisor	010810	Sterling
Physical	STHosting02	N/A - Internal	172.22.64.70	ESXI	Hypervisor	010811	Sterling
Physical	STHosting03	N/A - Internal	172.22.64.65	ESXI	Hypervisor	010744	Sterling
Physical	STHosting04	N/A - Internal	172.22.64.94	ESXI	Hypervisor	1235	Sterling
Physical	STHosting05	N/A - Internal	172.22.64.99	ESXI	Hypervisor	1237	Sterling

TYPE	NAME	DNS NAME	IP ADDRESS	GUEST OS	SEER*DMS COMPONENT	ASSET TAG	LOCATION (Common Name)
Physical	red	ssl3.imsweb.com	144.202.238.157	Check Point	Firewall, VPN, and IPS	010292	Baltimore
Physical	orange	ssl3.imsweb.com	144.202.238.157	Check Point	Firewall, VPN, and IPS	010293	Baltimore
Physical	purple	ssl4.imsweb.com	131.226.201.233	Check Point	Firewall, VPN, and IPS	010498	Sterling
Physical	violet	ssl4.imsweb.com	131.226.201.233	Check Point	Firewall, VPN, and IPS	010499	Sterling
Physical	cardinal-01	N/A - Internal	172.22.70.5	NetApp CDOT	Data Storage Services	010791	Sterling
Physical	cardinal-02	N/A - Internal	172.22.70.5	NetApp CDOT	Data Storage Services	010801	Sterling
Physical	cardinal-03	N/A - Internal	172.22.70.5	NetApp CDOT	Data Storage Services	1249	Sterling
Physical	cardinal-04	N/A - Internal	172.22.70.5	NetApp CDOT	Data Storage Services	1323	Sterling
Physical	oriole-01	N/A - Internal	172.22.16.7	NetApp CDOT	Data Storage Services	010790	Baltimore
Physical	oriole-02	N/A - Internal	172.22.16.7	NetApp CDOT	Data Storage Services	010792	Baltimore
Physical	oriole-03	N/A - Internal	172.22.16.7	NetApp CDOT	Data Storage Services	1247	Baltimore
Physical	oriole-04	N/A - Internal	172.22.16.7	NetApp CDOT	Data Storage Services	1248	Baltimore
Physical	pure-01	N/A - Internal	172.22.16.55	Purity	Data Storage Services	010485	Baltimore
Physical	pure-02	N/A - Internal	172.22.16.55	Purity	Data Storage Services	010487	Baltimore

TYPE	NAME	DNS NAME	IP ADDRESS	GUEST OS	SEER*DMS COMPONENT	ASSET TAG	LOCATION (Common Name)
Physical	pure-st-01	N/A - Internal	172.22.64.34	Purity	Data Storage Services	010657	Sterling
Physical	pure-st-02	N/A - Internal	172.22.64.34	Purity	Data Storage Services	010658	Sterling
Physical	Summit-BTP-Core	N/A - Internal	172.22.16.1	Extreme Networks	Network and switching	010482	Baltimore
Physical	Summit-BTP-Hosting	N/A - Internal	144.202.234.1	Extreme Networks	Network and switching	1203	Baltimore
Physical	Summit-BTP-Layer2	N/A - Internal	172.22.16.3	Extreme Networks	Network and switching	010195	Baltimore
Physical	Summit-ST-Core	N/A - Internal	172.22.64.1	Extreme Networks	Network and switching	1325	Sterling
Physical	Summit-ST-Hosting	N/A - Internal	172.22.64.67	Extreme Networks	Network and switching	1204	Sterling
Physical	Summit-ST-Layer2	N/A - Internal	131.226.202.4	Extreme Networks	Network and switching	010180	Sterling

3.2.3 Virtual Resources

TYPE	NAME	DNS NAME	IP ADDRESS	GUEST OS	SEER*DMS COMPONENT	LOCATION (Common Name)
	For each registry: xx = abbreviation					
Virtual	xxseerdms-pg-prod	xxseerdms-pg-prod.seerdms.com	both public and private	CentOS 7	Production database (Postgres) server	Both co-location facilities
Virtual	xxseerdms-app-prod	xxseerdms-app-prod.seerdms.com	both public and private	CentOS 7	Production application (WildFly) server	Both co-location facilities
Virtual	xxseerdms-pg-test	xxseerdms-pg-test.seerdms.com	both public and private	CentOS 7	Non-production database (Postgres) server	Both co-location facilities
Virtual	xxseerdms-app-test	xxseerdms-app-test.seerdms.com	both public and private	CentOS 7	Non-production application (WildFly) server	Both co-location facilities

3.3 Step 3: Identify Recovery Priorities for System Resources

The table below lists the order of recovery for the SEER*DMS resources. The table also identifies the expected time for recovering the resource following a "worst case" (complete rebuild/repair or replacement) disruption.

Priority	SEER*DMS Component	Worst Case Recovery
1	IMS firewall, VPN, and IPS	48 hours
2	Production: Postgres server	48 hours
3	Production: application/web server	48 hours
4	Test, alpha, and beta tiers: Postgres server	2 weeks
5	Test, alpha, and beta tiers: application/web server	2 weeks

These also include the time necessary to recover lost data. Virtual machines and content recovery activities would take place in the surviving co-location facility where capacity already exists. No work on repairing or replacing hardware would take place until the SEER*DMS users are back to work. A completely functional IMS firewall, VPN, and IPS already exists in the surviving co-location facility.

END OF DOCUMENT

Schedule G - Federal Provisions Addendum

This addendum applies to purchases that will be paid for in whole or in part with funds obtained from the federal government. The provisions below are required, and the language is not negotiable. If any provision below conflicts with the State's terms and conditions, including any attachments, schedules, or exhibits to the State's Contract, the provisions below take priority to the extent a provision is required by federal law; otherwise, the order of precedence set forth in the Contract applies. Hyperlinks are provided for convenience only; broken hyperlinks will not relieve Contractor from compliance with the law.

1. Equal Employment Opportunity

If this Contract is a "**federally assisted construction contract**" as defined in 41 CFR Part 60-1.3, and except as otherwise may be provided under 41 CFR Part 60, then during performance of this Contract, the Contractor agrees as follows:

(1) The Contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, or national origin. The Contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment without regard to their race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following:

Employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided setting forth the provisions of this nondiscrimination clause.

(2) The Contractor will, in all solicitations or advertisements for employees placed by or on behalf of the Contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.

(3) The Contractor will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This provision shall not apply to instances in which an employee who has access to the compensation information of other employees or applicants as a part of such employee's essential job functions discloses the compensation of such other employees or applicants to individuals who do not otherwise have access to such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with the Contractor's legal duty to furnish information.

(4) The Contractor will send to each labor union or representative of workers with which he has a collective bargaining agreement or other contract or understanding, a notice to be provided advising the said labor union or workers' representatives of the Contractor's commitments under this section and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

(5) The Contractor will comply with all provisions of Executive Order 11246 of September 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.

(6) The Contractor will furnish all information and reports required by Executive Order 11246 of September 24, 1965, and by rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the administering agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.

(7) In the event of the Contractor's noncompliance with the nondiscrimination clauses of this contract or with any of the said rules, regulations, or orders, this Contract may be canceled, terminated, or suspended in whole or in part and the Contractor may be declared ineligible for further Government contracts or federally assisted construction contracts in accordance with procedures authorized in Executive Order 11246 of September 24, 1965, and such other sanctions may be imposed and remedies invoked as provided in Executive Order 11246 of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.

(8) The Contractor will include the portion of the sentence immediately preceding paragraph (1) and the provisions of paragraphs (1) through (8) in every subcontract or purchase order unless exempted by rules,

regulations, or orders of the Secretary of Labor issued pursuant to section 204 of Executive Order 11246 of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. The Contractor will take such action with respect to any subcontract or purchase order as the administering agency may direct as a means of enforcing such provisions, including sanctions for noncompliance:

> Provided, however, that in the event a Contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction by the administering agency, the Contractor may request the United States to enter into such litigation to protect the interests of the United States.
>
> The applicant further agrees that it will be bound by the above equal opportunity clause with respect to its own employment practices when it participates in federally assisted construction work: *Provided,* that if the applicant so participating is a State or local government, the above equal opportunity clause is not applicable to any agency, instrumentality or subdivision of such government which does not participate in work on or under the contract.
>
> The applicant agrees that it will assist and cooperate actively with the administering agency and the Secretary of Labor in obtaining the compliance of contractors and subcontractors with the equal opportunity clause and the rules, regulations, and relevant orders of the Secretary of Labor, that it will furnish the administering agency and the Secretary of Labor such information as they may require for the supervision of such compliance, and that it will otherwise assist the administering agency in the discharge of the agency's primary responsibility for securing compliance.
>
> The applicant further agrees that it will refrain from entering into any contract or contract modification subject to Executive Order 11246 of September 24, 1965, with a contractor debarred from, or who has not demonstrated eligibility for, Government contracts and federally assisted construction contracts pursuant to the Executive Order and will carry out such sanctions and penalties for violation of the equal opportunity clause as may be imposed upon contractors and subcontractors by the administering agency or the Secretary of Labor pursuant to Part II, Subpart D of the Executive Order. In addition, the applicant agrees that if it fails or refuses to comply with these undertakings, the administering agency may take any or all of the following actions: Cancel, terminate, or suspend in whole or in part this grant (contract, loan, insurance, guarantee); refrain from extending any further assistance to the applicant under the program with respect to which the failure or refund occurred until satisfactory assurance of future compliance has been received from such applicant; and refer the case to the Department of Justice for appropriate legal proceedings.

2. Davis-Bacon Act (Prevailing Wage)

If this Contract is a **prime construction contracts** in excess of $2,000, the Contractor (and its Subcontractors) must comply with the Davis-Bacon Act (40 USC 3141-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, “Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction”), and during performance of this Contract the Contractor agrees as follows:

(1) All transactions regarding this contract shall be done in compliance with the Davis-Bacon Act (40 U.S.C. 3141- 3144, and 3146-3148) and the requirements of 29 C.F.R. pt. 5 as may be applicable. The contractor shall comply with 40 U.S.C. 3141-3144, and 3146-3148 and the requirements of 29 C.F.R. pt. 5 as applicable.

(2) Contractors are required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor.

(3) Additionally, contractors are required to pay wages not less than once a week.

3. Copeland “Anti-Kickback” Act

If this Contract is a contract for construction or repair work in excess of $2,000 where the Davis-Bacon Act applies, the Contractor must comply with the Copeland “Anti-Kickback” Act (40 USC 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, “Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States”), which prohibits the Contractor and subrecipients from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled, and during performance of this Contract the Contractor agrees as follows:

(1) Contractor. The Contractor shall comply with 18 U.S.C. § 874, 40 U.S.C. § 3145, and the requirements of 29 C.F.R. pt. 3 as may be applicable, which are incorporated by reference into this contract.

(2) Subcontracts. The Contractor or Subcontractor shall insert in any subcontracts the clause above and such other clauses as FEMA or the applicable federal awarding agency may by appropriate instructions require, and also a clause requiring the Subcontractors to include these clauses in any lower tier subcontracts. The prime contractor shall be responsible for the compliance by any subcontractor or lower tier subcontractor with all of these contract clauses.

(3) Breach. A breach of the contract clauses above may be grounds for termination of the contract, and for debarment as a Contractor and Subcontractor as provided in 29 C.F.R. § 5.12.

4. Contract Work Hours and Safety Standards Act

If the Contract is **in excess of $100,000** and **involves the employment of mechanics or laborers**, the Contractor must comply with 40 USC 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5), as applicable, and during performance of this Contract the Contractor agrees as follows:

(1) Overtime requirements. No Contractor or Subcontractor contracting for any part of the contract work which may require or involve the employment of laborers or mechanics shall require or permit any such laborer or mechanic in any workweek in which he or she is employed on such work to work in excess of forty hours in such workweek unless such laborer or mechanic receives compensation at a rate not less than one and one-half times the basic rate of pay for all hours worked in excess of forty hours in such workweek.

(2) Violation; liability for unpaid wages; liquidated damages. In the event of any violation of the clause set forth in paragraph (1) of this section the Contractor and any Subcontractor responsible therefor shall be liable for the unpaid wages. In addition, such Contractor and Subcontractor shall be liable to the United States (in the case of work done under contract for the District of Columbia or a territory, to such District or to such territory), for liquidated damages. Such liquidated damages shall be computed with respect to each individual laborer or mechanic, including watchmen and guards, employed in violation of the clause set forth in paragraph (1) of this section, in the sum of $27 for each calendar day on which such individual was required or permitted to work in excess of the standard workweek of forty hours without payment of the overtime wages required by the clause set forth in paragraph (1) of this section.

(3) Withholding for unpaid wages and liquidated damages. The State shall upon its own action or upon written request of an authorized representative of the Department of Labor withhold or cause to be withheld, from any moneys payable on account of work performed by the Contractor or Subcontractor under any such contract or any other Federal contract with the same prime contractor, or any other federally-assisted contract subject to the Contract Work Hours and Safety Standards Act, which is held by the same prime contractor, such sums as may be determined to be necessary to satisfy any liabilities of such contractor or subcontractor for unpaid wages and liquidated damages as provided in the clause set forth in paragraph (2) of this section.

(4) Subcontracts. The Contractor or Subcontractor shall insert in any subcontracts the clauses set forth in paragraph (1) through (4) of this section and also a clause requiring the Subcontractors to include these clauses in any lower tier subcontracts. The prime contractor shall be responsible for compliance by any subcontractor or lower tier subcontractor with the clauses set forth in paragraphs (1) through (4) of this section.

5. Rights to Inventions Made Under a Contract or Agreement

If the Contract is funded by a federal “funding agreement” as defined under 37 CFR §401.2 (a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding agreement," the recipient or subrecipient must comply with 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

6. Clean Air Act and the Federal Water Pollution Control Act

If this Contract is **in excess of $150,000,** the Contractor must comply with all applicable standards, orders, and regulations issued under the Clean Air Act (42 USC 7401-7671q) and the Federal Water Pollution Control Act (33 USC 1251-1387), and during performance of this Contract the Contractor agrees as follows:

Clean Air Act

1. The Contractor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S.C. § 7401 et seq.
2. The Contractor agrees to report each violation to the State and understands and agrees that the State will, in turn, report each violation as required to assure notification to the Federal Emergency Management Agency or the applicable federal awarding agency, and the appropriate Environmental Protection Agency Regional Office.
3. The Contractor agrees to include these requirements in each subcontract exceeding $150,000 financed in whole or in part with Federal assistance provided by FEMA or the applicable federal awarding agency.

Federal Water Pollution Control Act

(1) The Contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. 1251 et seq.

(2) The Contractor agrees to report each violation to the State and understands and agrees that the State will, in turn, report each violation as required to assure notification to the Federal Emergency Management Agency or the applicable federal awarding agency, and the appropriate Environmental Protection Agency Regional Office.

(3) The Contractor agrees to include these requirements in each subcontract exceeding $150,000 financed in whole or in part with Federal assistance provided by FEMA or the applicable federal awarding agency.

7. Debarment and Suspension

A "contract award" (see 2 CFR 180.220) must not be made to parties listed on the government-wide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (51 FR 6370; February 21, 1986) and 12689 (54 FR 34131; August 18, 1989), "Debarment and Suspension." SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.

(1) This Contract is a covered transaction for purposes of 2 C.F.R. pt. 180 and 2 C.F.R. pt. 3000. As such, the Contractor is required to verify that none of the Contractor's principals (defined at 2 C.F.R. § 180.995) or its affiliates (defined at 2 C.F.R. § 180.905) are excluded (defined at 2 C.F.R. § 180.940) or disqualified (defined at 2 C.F.R. § 180.935).

(2) The Contractor must comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C, and must include a requirement to comply with these regulations in any lower tier covered transaction it enters into.

(3) This certification is a material representation of fact relied upon by the State. If it is later determined that the contractor did not comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C, in addition to remedies available to the State, the Federal Government may pursue available remedies, including but not limited to suspension and/or debarment.

(4) The bidder or proposer agrees to comply with the requirements of 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C while this offer is valid and throughout the period of any contract that may arise from this offer. The bidder or proposer further agrees to include a provision requiring such compliance in its lower tier covered transactions.

8. Byrd Anti-Lobbying Amendment

Contractors who apply or bid for an award of **$100,000 or more** shall file the required certification in Exhibit 1 – Byrd Anti-Lobbying Certification below. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, officer or employee of Congress, or an employee of a Member of Congress in connection with obtaining any Federal contract, grant, or any other award covered by 31 U.S.C. § 1352. Each tier shall also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the recipient who in turn will forward the certification(s) to the awarding agency.

9. Procurement of Recovered Materials

Under 2 CFR 200.322, Contractors must comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act.

(1) In the performance of this contract, the Contractor shall make maximum use of products containing recovered materials that are EPA-designated items unless the product cannot be acquired—

a. Competitively within a timeframe providing for compliance with the contract performance schedule;

b. Meeting contract performance requirements; or

c. At a reasonable price.

(2) Information about this requirement, along with the list of EPA- designated items, is available at EPA's Comprehensive Procurement Guidelines web site, https://www.epa.gov/smm/comprehensive- procurement-guideline-cpg-program.

(3) The Contractor also agrees to comply with all other applicable requirements of Section 6002 of the Solid Waste Disposal Act.

10. Additional FEMA Contract Provisions.

The following provisions apply to purchases that will be paid for in whole or in part with funds obtained from the Federal Emergency Management Agency (FEMA):

(1) Access to Records. The following access to records requirements apply to this contract:

a. The Contractor agrees to provide the State, the FEMA Administrator, the Comptroller General of the United States, or any of their authorized representatives access to any books, documents, papers, and records of the Contractor which are directly pertinent to this contract for the purposes of making audits, examinations, excerpts, and transcriptions.

b. The Contractor agrees to permit any of the foregoing parties to reproduce by any means whatsoever or to copy excerpts and transcriptions as reasonably needed.

c. The Contractor agrees to provide the FEMA Administrator or his authorized representatives access to construction or other work sites pertaining to the work being completed under the contract.

d. In compliance with the Disaster Recovery Act of 2018, the State and the Contractor acknowledge and agree that no language in this contract is intended to prohibit audits or internal reviews by the FEMA Administrator or the Comptroller General of the United States.

(2) Changes.

See the provisions regarding modifications or change notice in the Contract Terms.

(3) DHS Seal, Logo, And Flags.

The Contractor shall not use the DHS seal(s), logos, crests, or reproductions of flags or likenesses of DHS agency officials without specific FEMA pre-approval.

(4) Compliance with Federal Law, Regulations, and Executive Orders.

This is an acknowledgement that FEMA financial assistance will be used to fund all or a portion of the contract. The Contractor will comply with all applicable Federal law, regulations, executive orders, FEMA policies, procedures, and directives.

(5) No Obligation by Federal Government.

The Federal Government is not a party to this contract and is not subject to any obligations or liabilities to the State, Contractor, or any other party pertaining to any matter resulting from the Contract."

(6) Program Fraud and False or Fraudulent Statements or Related Acts.

The Contractor acknowledges that 31 U.S.C. Chap. 38 (Administrative Remedies for False Claims and Statements) applies to the Contractor's actions pertaining to this contract.

Schedule F, Attachment 1 - Byrd Anti-Lobbying Certification

Contractor must complete this certification if the purchase will be paid for in whole or in part with funds obtained from the federal government and the purchase is greater than $100,000.

APPENDIX A, 44 C.F.R. PART 18 – CERTIFICATION REGARDING LOBBYING

Certification for Contracts, Grants, Loans, and Cooperative Agreements

The undersigned certifies, to the best of his or her knowledge and belief, that:

1. No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

2. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.

3. The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

The Contractor, Information Management Services, Inc. certifies or affirms the truthfulness and accuracy of each statement of its certification and disclosure, if any. In addition, the Contractor understands and agrees that the provisions of 31 U.S.C. Chap. 38, Administrative Remedies for False Claims and Statements, apply to this certification and disclosure, if any.

E-SIGNED by David Annett
on 2022-06-23 13:58:05 EDT

Signature of Contractor's Authorized Official

David Annett Vice President

Name and Title of Contractor's Authorized Official

2022-06-23 13:58:05 UTC

Date