

PARTICIPATION AGREEMENT

This Participation Agreement ("PA"), Contract ID# (XXXXX), contains the terms for the purchase and/or license of products and/or provision of services from Insert Supplier Name ("Supplier"), whose address is Insert Supplier Address, for the benefit of Business Unit/Entity ("Buyer"), whose address is Business Unit/Entity address. The Enterprise Master Services Agreement ("EMSA"), CID# (XXXXX), is incorporated into this PA. Capitalized terms used but not defined in this PA shall have the meanings given in the EMSA. For the avoidance of doubt, this PA, together with the incorporated terms of the EMSA (collectively referred to as the "Agreement"), forms a standalone agreement between the Supplier and Buyer.

1. Participation Agreement Exhibits

- 1.1. This PA includes the following exhibits, unless otherwise noted:

Do not delete exhibit number. Replace exhibit name with "Intentionally Omitted" if any exhibit below will not be used.

- 1.1.1. Exhibit 1a – Master Statement of Work ("MSOW") - Template
- 1.1.2. Exhibit 1b – MSOW Work Order - Template
- 1.1.3. Exhibit 2 – Statement of Work ("SOW") Template
- 1.1.4. Exhibit 3 – Rate Schedule - Template to SOW/MSOW (Time & Materials or Fixed Fee or Intentionally Omitted)
- 1.1.5. Exhibit 4 – Information Security Requirements
- 1.1.6. Exhibit 5 – Supplier Software License (To be added or Intentionally Omitted)
- 1.1.7. Exhibit 6 – Offshore Locations

2. Term of Participation Agreement

- 2.1. **Term.** This PA shall become effective on EFFECTIVE DATE ("Agreement Effective Date") and shall end on EXPIRATION DATE (such period referred to as the "Term"), except as otherwise provided herein.
- 2.2. **Performance.** Unless Buyer by its Contract Administrator (designated in a MSOW/SOW) agrees in writing to an extension of time, Supplier shall complete any performance due under this PA before the Term ends. If, at any time, Supplier concludes it will be unable to complete performance before the end of the Term, Supplier shall immediately give the Buyer's Contract Administrator a complete explanation of the facts and reasons.

3. Termination

- 3.1. **Termination for Convenience.** Buyer, but not Supplier, may terminate this PA or any MSOW/SOW governed by this PA, in whole or in part, for its sole convenience upon fifteen (15) days' prior written notice. Supplier shall be paid for Services satisfactorily provided or performed prior to the effective date of termination. In no event shall Supplier be paid for costs incurred, anticipated profit, or support services performed after the effective date of termination.
- 3.2. **Termination by Department of Health and Human Services.** Buyer may terminate this PA immediately if the Department of Health and Human Services ("HHS") finds that Supplier has failed to satisfactorily perform Services in accordance with terms of this PA or any MSOW/SOW governed by this PA.
- 3.3. **Termination for Change Control.** Supplier shall give Buyer prompt written notice of any announcement of a Change in Control of Supplier. Buyer may, at its option, terminate this PA upon receipt of such written notice. "Change in Control" shall be defined as (i) consolidation or merger of Supplier with or into any entity, (ii) sale, transfer or other disposition of all or substantially all of the assets of Supplier or (iii) acquisition by any entity, or group of entities acting in concert, of a controlling interest in Supplier. For purposes of this Section, "controlling interest" shall mean (A) beneficial ownership of twenty percent (20%) or more of the outstanding voting securities of the Supplier or (B) the right or power, whether by contract or otherwise, to direct Supplier's affairs or control Supplier's decisions, including without limitation the right or power to elect or appoint twenty percent (20%) or more of the board of directors or other persons in whom is vested decision-making authority for Supplier.

- 3.4. **Termination Effect on MSOW or SOW.** The termination of this PA will not affect any MSOW/SOW that, by its own terms, extends beyond the effective date of termination of this PA, and the parties will be bound by the terms of this PA until termination or expiration any MSOW/SOW governed by this PA. The expiration or earlier termination of this PA will not relieve, release or discharge either party hereto from any obligation, debt or liability that may have previously accrued and that remains to be performed as of the date of termination. The provisions of this section will survive the termination or expiration of this PA. Termination of this PA will be in addition to and not in lieu of any other remedies available to a party in law or in equity.
- 3.5. **Continued Performance.** Each party agrees to continue performing its obligations under this PA while any dispute is being resolved, except to the extent the issue in dispute precludes performance (dispute over payment shall not be deemed to preclude performance).
- 3.6. **Transition Assistance.** Upon expiration or termination of the Agreement for any reason, Supplier will, at Buyer's request, provide transition assistance services, as described in this Section, on the terms set forth in this Agreement at the then-current rates prior to expiration or termination of the Agreement. During a period of up to six (6) months after the termination or expiration of the Agreement, Supplier will cooperate with Buyer and its designees and provide the assistance reasonably requested by Buyer or its designee to allow Buyer's business operations to continue without material interruption or adverse effect and to facilitate the orderly transfer of responsibility for the Services then being provided by Supplier to Buyer or its designees, including, without limitation (a) continuing to provide the products, systems and/or perform the Services then being performed by Supplier; and (b) developing, with the assistance of Buyer or its designees, a plan for the transition of the products, systems and/or Services then being provided and/or performed by Supplier to Buyer or its designees.

4. Statements of Work and Services

- 4.1. **Services.** Assignments, tasks, products, functions or services provided by Supplier under this PA ("Services") shall be set forth in either a Master Statement of Work ("MSOW"), MSOW Work Order or a Statement of Work or other mutually agreed contract document ("SOW"), in formats substantially similar to Exhibit 1a,1b or 2. If any assignments, tasks, services, functions, or responsibilities are required for the proper performance and provision of the Services, regardless of whether they are specifically described herein, they shall be deemed to be implied by and included within the scope of the Services to be provided by Supplier to the same extent and in the same manner as if specifically described in this PA or the MSOW/MSOW Work Order or SOW. Buyer must agree in writing to the Services prior to Supplier's commencement of any work under a MSOW/MSOW Work Order or SOW. Supplier is a non-exclusive provider of the Services to Buyer, and Buyer may obtain similar services from other third parties. In providing the Services, Supplier shall provide all resources necessary for Supplier and its personnel to perform the Services (including personnel, software, tools, personal computers, hardware, circuits, equipment and facilities), except to the extent Supplier and Buyer agree otherwise in writing in a MSOW/MSOW Work Order or SOW. The Services shall be performed in a manner, sequence and timing so as to coordinate with the work of Buyer's contractors, suppliers and other consultants, if applicable, and Supplier agrees to cooperate in good faith with such third parties working on Buyer's behalf.
- 4.1.1. When Buyer engages Supplier on a Time and Materials basis under this PA, the following data elements will be provided: Role/Title, Hourly Rate (shall be set forth in Exhibit 3), Work Location, and Total Approved Amount. These data elements will be included in the SOW (the SOW will exclude the Resource Name). At its discretion, Buyer may choose to issue a SOW and STP Work Order or STP Work Order only. A Purchase Order will be issued for invoicing and administrative purposes. Changes in resources or adding funds to an executed SOW or STP Work Order will be completed by Buyer's Purchase Order only. Any other material changes to the SOW shall be documented in an amendment signed by both parties.
- 4.1.2. When Buyer engages Supplier in reference to the Fixed Fee Schedule in accordance with Exhibit 3, Buyer may choose to execute a MSOW/MSOW Work Order or SOW or issue a Purchase Order only. Any material changes to the MSOW/MSOW Work Order or SOW shall be documented in an amendment signed by both parties.

- 4.2. **Changes.** Supplier cannot make any changes to the Services without Buyer's prior written approval. Supplier must notify the Contract Administrator in writing within five (5) business days of Supplier's request for change to the MSOW/SOW. Supplier's request for a change to the Service(s) will include: (a) a detailed description of the change requested; (b) the business, technical, and financial justification for the change; (c) if known at the time the change request is made, the price and capital costs (if separate) associated with the change; (d) if known at the time the change request is made, the projected schedule for the change; (e) the priority of the change; and (f) if known at the time the change request is made, the change in ongoing or future pricing or fees, if any, resulting from such change. The parties shall promptly confer regarding the change request and Buyer will approve or reject the change.
- 4.3. **Export.** The parties will comply with all export laws and regulations of the United States, including for "deemed exports", and all export controls applicable thereunder. To the extent within Supplier's control and as part of its provision of Services, Supplier shall be responsible for, and shall coordinate and oversee, compliance with such export laws in respect of such items exported or imported hereunder.
- 4.4. **Entirety/Amendments.** This PA incorporates each MSOW/MSOW Work Order and SOW in its entirety. The parties agree that any MSOW/MSOW Work Order and SOW provision that is inconsistent with this PA shall be of no force or effect, shall be disregarded and the PA provision shall take precedence, unless the MSOW/MSOW Work Order and SOW expressly states otherwise. In order for a MSOW/MSOW Work Order and SOW to modify or amend the PA or EMSA with respect to a particular MSOW/MSOW Work Order and SOW, the modifying or amending term must be included within the "Override" section of the MSOW/MSOW Work Order and SOW and must list the specific term from the PA or EMSA that it is intended to override. Any such modifying or amending terms shall apply only to the MSOW/MSOW Work Order and SOW in which such deviations are contained.

5. Government Programs

- 5.1. Supplier agrees to comply with the Government Programs provisions applicable to Supplier, as revised from time to time. The current versions of the Government Programs provisions can be found by visiting the following sites: Government compliance, Government Language Long Form (PDF) (FDR Suppliers) <https://www.bcbsm.com/amslibs/content/dam/microsites/suppliers/documents/government-programs-requirements-long.pdf>; or Government Language Short Form (PDF) (Non-FDR Suppliers) <https://www.bcbsm.com/amslibs/content/dam/microsites/suppliers/documents/government-programs-requirements-short.pdf>; or Government Language Long Form (PDF) (FDR Suppliers-PDP) <https://www.bcbsm.com/amslibs/content/dam/microsites/suppliers/documents/government-programs-requirements-long-form-part-d.pdf>. The Government Programs provisions are incorporated into and made a part of this PA. Buyer shall provide Supplier written notice of any revision thereto, and the revised version shall replace and supersede any and all prior versions.

6. Federal Employee Program and E-Verify

- 6.1. Supplier agrees to comply with the Federal Employee Program ("FEP") Addendum ("FEP Addendum") provisions as revised from time to time, as applicable to Supplier. The current version thereof can be found by visiting the following site: <https://www.bcbsm.com/amslibs/content/dam/microsites/suppliers/documents/required-fep-contract-flow-down-provisions.pdf> (under "Government Compliance, Required FEP Contract Flow-Down Provisions (PDF)"), and is incorporated herein by reference.
- 6.2. The FEP Addendum is a subcontract of a federal procurement contract with the United States Office of Personnel Management ("OPM"). As such, the FEP Addendum is subject to certain federal procurement clauses, the obligations of which must "flow down" to the Supplier.
- 6.3. Buyer may amend the FEP Addendum to include new or revised DOL, FAR and FEHBAR Flow-Down Clauses required under the OPM contract by providing thirty (30) days prior written notice of such amendment. Supplier's signature is not required to make any such amendment effective.

7. Supplier Personnel and Subcontracting

- 7.1. Supplier shall utilize, to perform the Services, employees and Subcontractors (subject to Section 7.2 below) (collectively, "Supplier Personnel") who are properly educated, trained, experienced, and fully qualified for the Services they are to perform. Supplier Personnel shall be proficient in English. Supplier is responsible for having in place with all Supplier Personnel (either directly or indirectly through their respective employers) such agreements respecting intellectual property rights as are necessary to comply with Section 8 (Intellectual Property) below.
- 7.2. Supplier shall not subcontract its obligations under this PA to any third-party company, individual or Supplier affiliate (collectively, "Subcontractor") unless Supplier provides Buyer with written notice and Buyer subsequently provides written approval of such Subcontractors. Supplier agrees that (a) any Subcontractor shall comply with all terms and conditions of this PA in the same manner as Supplier; and (b) Supplier remains fully and unconditionally responsible for all Services and for the Subcontractors' compliance with this PA, including any applicable MSOW/SOW

8. Intellectual Property

- 8.1. **Reporting of Work Product.** For purposes of this PA, "Work Product" means all original materials, tangible or intangible work product, and deliverables developed, invented, discovered, created, authored, or otherwise originated (whether alone or jointly with others) under this PA. Supplier shall promptly disclose all Work Product to Buyer upon its development, invention, discovery, creation, authoring or origination.
- 8.2. **Ownership of Work Product.** Supplier agrees that all Work Product and all intellectual property rights therein shall be the sole and exclusive property of Buyer. Supplier agrees to assign and does hereby expressly assign and transfer to Buyer all right, title and interest worldwide in and to the Work Product and all intellectual property rights contained therein.
- 8.3. **Works for Hire.** All works of authorship forming Work Product shall be, to the extent possible, considered a "work made for hire" for Buyer under the United States Copyright Laws and are the sole and exclusive property of Buyer, and shall immediately vest in Buyer.
- 8.4. **Assignment.** To the extent that any such Work Product does not qualify as "work for hire" under applicable law, Supplier hereby irrevocably and exclusively assigns to Buyer all right, title and interest in and to all such Work Product, agrees to sign all necessary or appropriate documents to register the any intellectual property in the name of Buyer, and shall cause Supplier Personnel to assign, at the time of creation for the Work Product, without the right of any further consideration, all right, title and interest in or that they may have in such Work Product to Buyer.
- 8.5. **Pre-Existing Materials.** To the extent that the Work Product includes materials existing as of the effective date of this PA, or materials of Supplier's licensors ("Pre-Existing Materials"), Supplier hereby grants to Buyer a perpetual, royalty-free, paid-up, irrevocable, transferable, sublicensable, worldwide, non-exclusive right and license to use, execute, reproduce publicly perform, display, modify, improve, create derivative works of, distribute, transmit, import, make, have made, sell and offer to sell and otherwise exploit any Pre-Existing Materials, including all such modifications, improvements and derivative works thereof, solely to the extent such Pre-Existing Materials are incorporated in, combined with or otherwise necessary or useful to use or exploit the Work Product for any purposes or reasonably required in connection with Buyer's receipt of the Work Product. Notwithstanding the foregoing, Supplier shall not incorporate any Pre-Existing Materials in any Work Product without prior written permission of Buyer.
- 8.6. **Further Assistance.** Supplier shall, upon request of Buyer, promptly execute a specific assignment of title to Buyer and do anything else reasonably necessary to enable Buyer to secure for itself any patent, trade secret or other proprietary rights in the United States or other countries relating to the Work Product. Such documents shall be prepared by Buyer, at Buyer's expense, and Supplier shall be required to sign them only upon the request of Buyer. All materials produced under this PA shall be and shall remain the property of Buyer, whether, or not registered.

- 8.7. **Open-Source Software.** Supplier represents and warrants, and shall ensure that its Personnel warrant, that it will not supply to Buyer any Work Product that is based upon, incorporates, links to or otherwise relies on software code that is subject to an "open source" license, including without limitation the GNU General Public License or other licenses listed at www.opensource.org ("Open Source Software") without Buyer's prior written consent. Such consent may be granted or withheld in Buyer's sole and exclusive discretion and must include a separate indication of approval by Buyer's legal counsel.
- 8.8. **Third-Party Software.** If Supplier intends to develop a Deliverable in a manner that incorporates or requires Buyer to use any Third Party Materials in order to use such Deliverable, then Supplier will (i) provide Buyer with prior notice, specifying in reasonable detail the nature of the Deliverable's dependency on or use of the Third Party Materials, and (ii) provide Buyer with (for no additional cost or on such terms as may be acceptable to Buyer) a perpetual, irrevocable, royalty-free, non-exclusive right and license for Buyer to use the Third Party Materials in connection with the use of the Deliverable. "Third Party Materials" shall mean data, images, programming, computer code, graphics, text, or other materials made, conceived, or developed by third parties, other than Open-Source Software described in Section 5.7 above, that will be incorporated into the Deliverable(s) or used to make the Deliverables useful to Buyer.
- 8.9. **No Malicious Code.** Supplier represents and warrants that: (i) any Deliverables provided by Supplier, or its Personnel under this Agreement will not, at the time of installation, contain any Disabling Code; and (ii) Supplier and its Personnel shall not at any time intentionally or negligently introduce any Disabling Code to any of Buyer's or its customers' systems or to the Deliverables or any Work Product. In the event Supplier breaches this warranty, Supplier shall, at Buyer's option and in addition to such other rights as Buyer may have with respect thereto, take all steps necessary at Supplier's sole cost to remove the Disabling Code and assist Buyer at no additional charge in restoring any and all data or programming lost by Buyer or its customers, or the end users of either of them, as a result of such Disabling Code. "Disabling Code" shall mean any virus, worm, trap door, back door, timer, clock, counter or other code, limiting routine, instruction or design that would erase data or programming or otherwise cause its software to become inoperable or incapable of being used in the full manner for which it was designed and created, or which permit unauthorized access to the system or unauthorized changes to the software, its functionality, or its output. Disabling Code shall include, without limitation, any limitations that are triggered by: (a) the software being used or copied a certain number of times, or after the lapse of a certain period of time; (b) the software being installed on or moved to a central processing unit or system different from the central processing unit or system on which the software was originally installed; or (c) the occurrence or lapse of any similar triggering factor or event.
- 8.10. **Survival.** The obligations of this Section shall survive the termination or expiration of this Agreement.

9. Offshore

- 9.1. Supplier and any approved Subcontractor shall not provide any services or support of such services outside of the United States without the prior written consent of Buyer. This shall include, but is not limited to, any access or sending of confidential data, including Protected Health Information ("PHI") or Personally Identifiable Information ("PII"), as defined by the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"), to a location outside of the United States.
- 9.2. If Supplier desires to access, store, host, view, transfer, or exchange PHI/PII, Confidential information or financial data pursuant to the Services or support of such services outside the United States, Supplier shall complete a Non-Domestic Vendor Form and Offshore Locations Form and submit them to Buyer. If Buyer consents to receive offshore services, such consent will be documented within a MSOW, SOW and/or Purchase Order and shall be limited in scope to those services set forth in the Non-Domestic Vendor Form accepted by Buyer. If Supplier desires to modify any offshore locations, Supplier shall notify Buyer in writing and submit a new Non-Domestic Vendor Form and Offshore Locations Form for Buyer's approval.

10. Payment Terms

10.1. Payment terms are 2% 15/Net 60. Payment for a properly submitted invoice is due within 60 days after the invoice is received and approved by Buyer within the Oracle Supplier Portal. In the event Buyer makes payment on or before the 15th day after receiving the invoice, Buyer shall take a 2% discount from the invoice total as consideration for the prompt payment. Payment shall be considered made by Buyer on the date printed on the check or on the date Buyer transfers the invoice payment via electronic transfer method (e.g., EFT). In no event shall Buyer be liable to Supplier for any interest or late payment fees.

11. Annual Volume Discount

11.1. During the term of this PA, the following annual volume rebate shall apply:

11.2. If the YTD Contract Volume, defined below in subsection 11.4, is \$0 - \$499,999, then the rebate shall be 4%. If the YTD Contract Volume is \$500,000 or more, then the rebate shall be 6%.

11.3. The applicable volume rebate shall be applied by Supplier on an annual basis to all Services performed by Supplier when a specified volume is reached. Discounts are based on when the work was performed, not when invoices are received (for example, invoices received after January 1st for work performed prior to January 1st, fall into the discount structure of the year the work was performed).

11.4. The volume rebate shall be based on Buyer's total payments made and outstanding payables due for that calendar year ("YTD Contract Volume"). All amounts due to Buyer under this Section shall be paid in full by a check within one hundred twenty (120) days of the end of the just completed calendar year. Checks should be mailed to Blue Cross Blue Shield of Michigan, Attn: Accounts Payable, Mail Code 0811; 600 Lafayette East, Detroit, Michigan 48226. Supplier shall also email a copy of the annual volume discount check and/or invoice credit statement to the Contract Administrator and the procurement representative.

11.5. In the event Buyer is owed any amounts under this Section after the termination of this PA, Supplier shall pay Buyer the full amount owing by check no later than sixty (60) days after the date this PA is terminated.

11.6. Buyer is not required to purchase any specific volume of Services from Supplier during the term of this PA, and Buyer makes no commitment for any minimum volume, scope or value of the Services.

11.7. Supplier's obligations under this Section shall survive the term of this PA.

12. Diverse Supplier Requirements

12.1. Supplier agrees to comply with registering through the Tier II Diverse Supplier Portal and to report the use of diverse companies for its secondary spend. In addition, Supplier agrees to comply with a fifteen (15) percent diversity spend requirement throughout the term of this PA. All spend must be uploaded to the Tier II Diverse Supplier Portal on a quarterly basis according to program reporting guidelines. Supplier will receive an email from "supplier.io" to register for UniTier following the completion of this PA. Registration on the portal must be completed within ten (10) business days of signing this PA.

13. 508 Electronic Accessibility Compliance

13.1. Supplier agrees that if any of the Services being provided are a part of Buyer's health programs or activities provided through electronic means and/or information technology (e.g., website or mobile application), all content will be accessible to individuals with disabilities as required under Section 1557 of the Affordable Care Act and Section 508 of the Rehabilitation Act. Content must also meet the most current Web Content Accessibility Guidelines ("WCAG") 2 requirements.

14. Non-Solicitation of Employees

14.1. With the exception of generalized recruiting practices, including but not limited to responses to advertisements, internet postings and job fairs, should either party like to solicit an employee of the other party to apply for regular employment, the party shall contact the other party's designated representative to determine if the employee is interested in pursuing an offer. If the employee is interested, the soliciting party's representative shall work with the other party to set up any needed meetings.

15. Notices

15.1. The parties shall deliver any notice by U.S. first class overnight mail, or express overnight courier addressed to:

15.1.1. **To Buyer:** Attn: Contract Administrator, Corporate Procurement Department, Blue Cross Blue Shield of Michigan, 600 Lafayette East, Mail Code: 0625, Detroit, MI 48226.

15.1.2. **With Copies to:** Attn: Contract Manager, Contract Management Department, Office of the General Counsel, Blue Cross Blue Shield of Michigan, 600 Lafayette East, Mail Code: 1915, Detroit, Michigan 48226.

15.1.3. **If to Supplier:** Notices shall be sent to the address listed in the Recital section of this PA unless otherwise specified herein.

SIGNATURES

BUSINESS UNIT/ENTITY

By: _____

Name: _____

Title: _____

Date: _____

By: _____

Name: _____

Title: _____

Date: _____

SUPPLIER NAME

By: _____

Name: _____

Title: _____

Date: _____

EXHIBIT 1a (Template)
MASTER STATEMENT OF WORK
Project Name

This Master Statement of Work, for **Project Name**, Contract ID# (XXXXX), and any attachment(s) hereto ("MSOW"), is governed by the Enterprise Master Service Agreement ("EMSA"), CID # (XXXXX), and the Participation Agreement ("PA"), CID # (XXXXX), between **Insert Business Unit/Entity** ("Buyer") and **insert Supplier** ("Supplier"), effective **insert effective date of PA** (the EMSA and PA are collectively the "Agreement"). If any term or condition in this MSOW conflicts with any term or condition in the Agreement, the Agreement shall control, unless otherwise stated herein.

In consideration of Supplier and Buyer's mutual promises, Supplier agrees to perform this MSOW as follows:

I. Scope of Work and Project Deliverables

- A. Project Overview.** This MSOW describes the Services and key Deliverables on a general level to be performed and provided by Supplier for Buyer.
- B. MSOW Term.** This MSOW shall begin on _____, 20____ and shall end on _____, 20____ ("MSOW Term").
- C. Scope of Work**
- 1. Description of Services and Deliverables.** "Services" and "Deliverables" to be provided by Supplier will be defined and described in Exhibit 1b, "MSOW Work Order" (including, but not limited to, a breakdown of fees, expected volumes and project management requirements).
 - 2. Service Level Agreements ("SLAs").** Services provided under the MSOW Work Order will meet or exceed the SLA's defined in Exhibit 1b "MSOW Work Order." Supplier agrees to manage Services and Deliverables (including but not limited to resources and project requirements) against target dates allotted for each milestone and due date, as agreed to by the parties. Failure to meet required SLAs will be considered a material breach under the Agreement and Supplier shall be required to provide recourse for such breach as specified in the MSOW Work Order and fees shall incur.
- D. Termination.** If Buyer terminates this MSOW and does not expressly terminate the MSOW Work Order(s), the MSOW Work Order shall remain in full force and effect, and the terms of this MSOW shall survive with respect to such MSOW Work Order(s) only until the expiration or termination of such MSOW Work Order(s).
- E. Work Location.** All Services shall be performed within the United States or remotely within the United States.
- F. Subcontractors.** By executing the MSOW, Supplier attests its Subcontractors shall abide by all terms and conditions of this MSOW and the Agreement. Buyer consents to the following Subcontractors:

Name of Subcontractor	Services provided by Subcontractor

G. Warranties and Representations.

- 1. Supplier Services Warranty.** Supplier represents and warrants for **[12 months]** after receipt of final payment (i) the Services will be performed in a good and workmanlike manner, (ii) the Services will be performed by qualified personnel using reasonable diligence and care, and (iii) any Supplier applications will be performed substantially in accordance with their intended purpose and documentation.
- 2. Mutual Representations.** Each party represents to the other that (i) it has duly formed and in good standing, (ii) it has the requisite power and has taken all actions necessary to execute this Agreement and all SOWs; and (iii) this Agreement and each SOW when signed by each party shall constitute legal, valid and binding obligations of that party in accordance with its terms.

II. Pricing and Payment Terms

- A. **Pricing.** The pricing under this fixed fee MSOW shall be set forth within the applicable MSOW Work Order(s). For each requested Deliverable, Supplier shall provide Buyer with its pricing based on Buyer's specifications and incorporated into the applicable MSOW Work Order. Buyer may approve project funding by issuing a Purchase Order to Supplier.
- B. **Roles and Rates.** "Roles and Rates" are set in accordance with the PA and are listed as follows:

Role	Rate	Role	Rate
	\$		\$
	\$		\$

- C. **Changes.** Any changes in the Services and/or Deliverables under this MSOW will require written approval by Buyer including an amendment to the Agreement and/or MSOW, as applicable, in accordance with Section 4 of the PA.
- D. **Payment.** Buyer will approve and pay invoices based on the established payment terms in the Agreement.

III. Supplier Attestation

- A. By executing this MSOW, Supplier attests that as of the Supplier's signature date, Supplier is in compliance with the Government Programs provisions set forth in the Agreement, including all requirements relating to checking the OIG List and GSA List (as those terms are defined in the Agreement).

SIGNATURES

The above MSOW is agreed to by both parties as witnessed by their respective signatures below. By signing this MSOW, the signatory for each party hereby certifies and warrants that he or she has the actual authority to bind their respective party to this MSOW. Supplier acknowledges and attests that Services performed pursuant to this MSOW by it or its third-party subcontractors shall ONLY be performed at remote locations within the United States.

BUYER

By: _____

Name: _____

Title: _____

Date: _____

By: _____

Name: _____

Title: _____

Date: _____

SUPPLIER

By: _____

Name: _____

Title: _____

Date: _____

EXHIBIT 1b (Template)
MASTER STATEMENT OF WORK
WORK ORDER #
Project Name

This is MSOW Work Order # is for **Insert Project Name**, which includes any attachments hereto, is governed by the Master Statement of Work, CID# (**Insert CID # of MSOW**) between **Business Unit/Entity** ("Buyer") and **Supplier Name** ("Supplier"), effective **insert effective date of MSOW** ("MSOW"). This MSOW Work Order and the MSOW are subject to the terms and conditions of the Enterprise Master Service Agreement ("EMSA"), CID# (**XXXXX**), and the Participation Agreement ("PA"), CID# (**XXXXX**). The EMSA and PA are collectively referred to as the "Agreement". Capitalized terms that are used, but not defined in this MSOW Work Order, will have the meanings given in the MSOW and the Agreement. If any term or condition in this MSOW Work Order conflicts with any term or condition in the MSOW, the MSOW shall control.

In consideration of Supplier's and Buyer's mutual promises, Supplier agrees to perform this MSOW Work Order as follows:

I. Scope of Services and Project Deliverables

- A. Project Overview.** This MSOW Work Order defines and describes the Services and Deliverables to be performed and provided by Supplier for Buyer.
- B. MSOW Work Order Term.** This MSOW Work Order shall begin **_____**, 20**__** and end **on _____**, 20**__** unless otherwise terminated in accordance with the Agreement. This MSOW Work Order describes the Services and Deliverables to be performed and priced by the Supplier for Buyer.
- C. Scope of Work.**

- 1. Description of Services and Deliverables.** Services are defined and shall be performed by the Supplier as follows, and shall yield the following Deliverables: [Insert]

Services	Deliverables	Milestones

- D. Work Location.** Services shall be performed within the United States at the following locations **Insert work locations**. Any Services performed remotely shall be completed within the United States. Non-domestic locations are not accepted for this MSOW Work Order.

- II. Service Level Agreements ("SLA's").** Services provided under this MSOW Work Order will meet or exceed the following service levels:

Definition	Measurement	Time Period	Penalty

III. Fees, Payment Terms and Conditions

- A. Pricing Schedule.** Pricing for this fixed fee MSOW Work Order shall be as follows:

Milestone	Deliverables	Payment	Deliverable Due Date
Total			

- B. Total Amount of the MSOW Work Order.** The total billable amount of the MSOW Work Order shall not exceed \$ U.S. Dollars.
- C. Final Inspection and Acceptance.** Buyer shall inspect all Services and Deliverables completed by Supplier under this MSOW Work Order. The Contract Administrator must provide written acceptance that the Services and Deliverables have been completed by Supplier as required under this MSOW Work Order. If the completed Services and Deliverables have not been accepted by the Contract Administrator, Supplier agrees to provide all necessary materials, permits, and services required at no additional cost to Buyer until the Contract Administrator provides written acceptance.

IV. Buyer Administrative Details

- A. Contract Administrator.** Buyer will designate a Contract Administrator for this MSOW Work Order and reserves the right to change such Contract Administrator at its discretion. Buyer shall provide Supplier written notice of any changes to the Contract Administrator.
- B. Purchase Order Number.** Buyer shall assign a Purchase Order number associated with the MSOW Work Order after the execution of this MSOW Work Order for administrative and invoicing purposes. All Supplier invoices shall include the assigned Purchase Order number. Failure to include the assigned Purchase Order number on an invoice relieves Buyer of its payment obligations under this MSOW Work Order until Buyer remedies such failure.
- C. Invoices.** All invoices shall be submitted for actual costs through the Oracle Supplier Portal against the assigned Purchase Order number to the MSOW Work Order.
- D. Roster.** Supplier shall submit a new Resource Roster as provided by Buyer, including any changes to Supplier personnel to: Contingentlabor@bcbsm.com no later than seven (7) days prior to the effective date of the change.

SIGNATURES

This MSOW Work Order is agreed to by both parties as witnessed by their respective signatures below. By signing this MSOW Work Order, the signatory for each party hereby certifies and represents that he or she has the actual authority to bind their respective party to this MSOW Work Order. Supplier acknowledges and attests that Services performed pursuant to this MSOW Work Order by it or its third-party subcontractors shall ONLY be performed at remote locations within the United States.

BUYER

By: _____

Name: _____

Title: _____

Date: _____

By: _____

Name: _____

Title: _____

Date: _____

SUPPLIER

By: _____

Name: _____

Title: _____

Date: _____

EXHIBIT 2 (Template)
STATEMENT OF WORK ##-####
Project Name

This Statement of Work #XX-XXXXX, Contract ID# (XXXXX), and any attachment(s) hereto ("SOW"), is governed by the Enterprise Master Service Agreement ("EMSA"), CID# (XXXXX), and the Participation Agreement ("PA"), CID# (XXXXX) or insert Master Agreement, CID# (XXXXX), between Business Unit/Entity ("Buyer") and Supplier Name ("Supplier"), effective insert effective date of Master Agreement or PA ("Agreement"). If any term or condition in this SOW conflicts with any term or condition in the Agreement, the Agreement shall control.

In consideration of Suppliers and Buyer's mutual promises, Supplier agrees to perform this SOW as follows:

I. Scope of Work and Project Deliverables

A. Project Overview. This SOW describes the Services and key Deliverables on a general level to be performed and provided by Supplier for Buyer (Contract Administrator to include a 2-3 sentence summary of the SOW)

B. SOW Term. This SOW shall begin _____, 20____, and shall end _____, 20____ ("SOW Term").

C. Scope of Work.

- 1. Description of Services and Deliverables.** "Services" and "Deliverables" are defined and shall be performed/provided by the Supplier as follows (including, but not limited to, a breakdown of fees, expected volumes and project management requirements):

Supplier Services	Deliverables

- 2. Service Level Agreements "SLA".** Services provided under this SOW will meet or exceed the following service levels:

Definition	Measurement	Time Period	Penalty

- a. Failure to meet required SLAs will be considered a material breach under the Agreement and Supplier shall be required to provide recourse for such breach as specified in the SOW and fees shall incur.

D. Work Location. Services provided under this SOW shall be performed by Supplier's resources at: list exact work location address. If work will be performed remotely, specify remote location. (Ex: Remotely within the United States)

E. Subcontractors. By executing the SOW, Supplier attests its Subcontractors shall abide by all terms and conditions of this SOW and the Agreement. Buyer consents to the following Subcontractors.

Name of Subcontractor	Services provided by Subcontractor	Subcontractor Offshore Services

F. Warranties and Representations.

- 1. Supplier Services Warranty.** Supplier represents and warrants for [12 months] after receipt of final payment (i) the Services will be performed in a good and workmanlike manner, (ii) the Services will be performed by qualified personnel using reasonable diligence and care, and (iii) any Supplier applications will be performed substantially in accordance with their intended purpose and documentation.

2. **Mutual Representations.** Each party represents to the other that (i) it has duly formed and in good standing, (ii) it has the requisite power and has taken all actions necessary to execute this Agreement and all SOWs; and (iii) this Agreement and each SOW when signed by each party shall constitute legal, valid and binding obligations of that party in accordance with its terms.

II. Payment and Payment Milestone Conditions

- A. **Pricing Schedule.** The pricing for this Fixed Fee SOW or Time and Materials SOW shall be as follows:

Milestone	Deliverables	Payment	Deliverable Due Date
Total			

- B. **Total Amount of SOW.** The total billable amount of this SOW shall not exceed \$ U.S. Dollars. The parties agree to a change in fees in accordance with Section 4.2 of the PA.
- C. **Final Inspection and Acceptance.** Buyer shall inspect all Services and Deliverables completed by Supplier under this SOW. The Contract Administrator must provide written acceptance that the Services and Deliverables have been completed by Supplier as required under this SOW. If the completed Services and Deliverables have not been accepted by the Contract Administrator, Supplier agrees to provide all necessary materials, permits, and services required at no additional cost to Buyer until the Contract Administrator provides written acceptance.

III. Buyer Administrative Details

- A. **Contract Administrator.** Buyer will designate a Contract Administrator for this SOW and reserves the right to change such Contract Administrator at its discretion. Buyer shall provide Supplier written notice of any changes to the Contract Administrator.
- B. **Purchase Order Number.** Buyer shall assign a Purchase Order number after the execution of this SOW for administrative and invoicing purposes. All Supplier invoices shall include the assigned Purchase Order number. Failure to include the assigned Purchase Order relieves Buyer of its payment obligations under this PA until such failure has been remedied.
- C. **Invoices.** All Invoices shall be submitted through the Oracle Supplier Portal against the assigned Purchase Order number to this SOW and shall be emailed to the Contract Administrator.

IV. Supplier Attestation

- A. By executing this SOW, Supplier attests that as of the effective date of this SOW Supplier is in compliance with the Government Programs provisions set forth in the Agreement, including all requirements relating to checking the OIG List and GSA List (as those terms are defined in the Agreement).

Keep subsections 1-3 below for a Time and Materials SOW or DELETE the following subsections 1-3 if this SOW is for Fixed Fee.

1. Buyer may generate an electronic invoice in its STP system on behalf of Supplier for the service(s) performed by first Wednesday of the month following the preceding financial month based on the Supplier's invoice cycling date. Buyer shall approve and pay the invoice based on the established payment terms and the current calendar year invoicing schedule with Supplier. If timesheet submission is required in the applicable time reporting tools, invoices will be created based off the approved time and paid in accordance with your payment terms.
2. **Professional Fees.** The Services under this SOW shall be performed in accordance with the following Roles and Hourly Rate(s). Changes to any role or rate below requires written approval by the Buyer's Contract Administrator and an Amendment to this SOW.

Role/Title	Hourly Rate
EXAMPLE: Consultant, Advanced	\$

3. **Insert Roster Language.** The Services under this SOW shall be performed on a time and materials basis in accordance with the billable rates and hours detailed in the Resource Roster for this SOW. Supplier shall complete the initial Resource Roster prior to execution of this SOW. Changes to the Resource Roster requires written approval by the Buyer Contract Administrator and Supplier. Buyer Contract Administrator, or Delivery Lead shall submit a new Resource Roster including the changes to Supplier Personnel to Contingent Labor Contingentlabor@bcbsm.com no later than seven (7) days prior to the effective date of the change. Buyer is not liable to pay for any labor performed by Supplier Personnel not on a fully approved Resource Roster on or before the resources start date. Resources that are not included on this Resource Roster shall not be entered into Buyer's time reporting tool (STP or other).

SIGNATURES

This SOW is agreed to by both parties as witnessed by their respective signatures below. By signing this SOW, the signatory for each party hereby certifies and warrants that he or she has the actual authority to bind their respective party to this SOW. Supplier acknowledges and attests that Services performed pursuant to this SOW by it or its third-party subcontractors shall ONLY be performed at remote locations within the United States.

BUYER

By: _____

Name: _____

Title: _____

Date: _____

By: _____

Name: _____

Title: _____

Date: _____

SUPPLIER

By: _____

Name: _____

Title: _____

Date: _____

RATE SCHEDULE

TIME & MATERIALS or FIXED FEE (select the title and section that applies)

Time & Materials

The Services under the Statement of Work (SOW) shall be performed in accordance with the following Roles and Hourly Rate(s), and Resource's Location (onshore/Offshore). Changes to any role or rate below requires written approval by the Buyer Contract Administrator and an Amendment to the SOW.

Buyer and Supplier agree to the following Rate Schedule, which sets forth the rates per hour for each Supplier resource level delivering Services. Supplier's rates, as of the Effective Date, and/or as amended, are referred to as the "Rates". This Rate Schedule is made effective upon the execution of the Agreement and shall remain in effect until the termination of the Agreement; or until an adjusted Rate Schedule is agreed to in writing by both parties. Any adjustment to the Rate Schedule must be mutually agreed to, in writing, by Buyer's Corporate Procurement Department and Supplier, and shall not become effective until signed by Buyer's Corporate Contract Administrator in the form of an Amendment to this Agreement. All Rate Schedule Amendments shall be numbered sequentially and contain the heading "Rate Schedule Amendment # ____" and indicate the effective dates. Buyer shall pay Supplier on a monthly basis for all Services completed during the prior month and approved by Buyer's Contract Administrator. Changes during the term of the controlling Agreement shall be set forth in the Rate Schedule through an Amendment and reflected below.

Role/Title	Hourly Rate	Resource Location Offshore (Y/N)
	\$	

OR

Fixed Fee

The Services under the Master Statement of Work (MSOW)/WO or Statement of Work (SOW) shall be performed in accordance with the following Description of Service(s) and Rate(s), and Work Location (must be onshore within the United States). Changes to any Description of Service or Rate below requires written approval by the Buyer Contract Administrator and an Amendment to the MSOW/WO or SOW. Changes during the term of the controlling Agreement shall be set forth in the Rate Schedule through an Amendment and reflected below.

Description of Service(s)	Rate
	\$

INFORMATION SECURITY REQUIREMENTS

1 Purpose

- 1.1 This Information Security Requirements document describes the minimum information security requirements that Supplier shall comply with in performing services for, or otherwise accessing Buyer data. All capitalized terms not defined in this Exhibit 4 shall have the meaning set forth in the PA.

2 Information Security Management Program & Policies

- 2.1 Supplier shall: (a) have an Information Security Management Program ("ISMP") that addresses the overall security program of Supplier's organization; (b) formally implement and document the ISMP; and (c) protect, control, and retain all ISMP records according to federal, state, and internal requirements.
- 2.2 During the Term of the Agreement and for so long as the Supplier retains BCBSM confidential data after termination, Buyer shall have the right to assess the maturity of the ISMP by reviewing Supplier's information security policies, audit results, analysis of monitored events, preventive measures, and corrective action plans at least annually.
- 2.3 Supplier shall develop, publish, and maintain information security policy documentation. The information security policy documentation shall include the purpose and scope of the policy, describe management's and workforce member's roles and responsibilities, and set forth Supplier's approach to establishing information security. The policy documents shall be reviewed no less than annually and updated as needed to ensure policies are current and operationally effective.

3 Access Management

- 3.1 Supplier shall develop, publish, and maintain formal access control policies to enforce business and security requirements for access management. Access management policies shall account for Supplier's logical and physical controls. Supplier shall review the policy documents no less than annually and update as needed to ensure policies are current and operationally effective.
- 3.2 Supplier shall develop, implement, and maintain a documented user registration and de-registration procedure for granting and revoking access. Supplier shall identify user account types, roles, and groups and establish requirements for membership. Supplier shall regularly review all access privileges of Supplier employees, contractors, and third-party users as required by Supplier's access management policies through a formal documented access review process.
- 3.3 Supplier shall require users to have unique identifiers for individual access use only. Supplier shall implement authentication and authorization mechanisms for information system and equipment access to verify users' identities.
- 3.3.1 Supplier shall restrict and control the use of access privileges to information systems and services through a formal documented authorization process. Supplier will only grant users the minimum necessary access privileges for performance of such user's specific job roles and responsibilities.
- 3.3.2 Supplier shall ensure access rights of all employees, contractors, and third-party users to Buyer's information and information assets shall be removed upon termination of their employment. Supplier shall ensure any changes of employment or other workforce arrangements shall result in a removal of all access rights or modification of access rights that are not required for the new employment or workforce arrangement.
- 3.3.3 Suppliers shall ensure that passwords are controlled through a formal management process. Supplier shall make users aware of their responsibilities for maintaining effective access controls and shall be required to follow good security practices in the selection and use of strong passwords.
- 3.3.4 Supplier shall implement secure authentication methods to control access of remote users to systems containing sensitive information by requiring the use of multifactor authentication mechanisms.

3.4 Supplier shall specify the networks and network services to which users are authorized to access. Users shall only be provided with access to internal and external network services that they have been specifically authorized to use. Supplier shall restrict the capability of users to connect to shared networks in line with Supplier's access control policy and requirements of its business applications.

3.4.1 Groups of information services, users and information systems shall be segregated on networks.

3.4.2 Supplier shall implement and maintain firewalls and intrusion detection and prevention systems, which will forward event data and security alerts to a centralized system information and event monitoring ("SIEM") system for analysis, reporting and incident response. Supplier shall perform firewall configuration and access control list reviews on at least a monthly basis, to ensure appropriate controls and configurations are applied to limit traffic to only what is required for business operations within networks such as internal, external, and any demilitarized zone (DMZ).

4 Human Resources Security Policies

4.1 Supplier shall define and document the security roles and responsibilities of employees, contractors, and third-party users in accordance with Supplier's information security policy.

4.2 Supplier shall ensure that employees, contractors, and third-party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to Buyer's data.

4.2.1 Supplier shall conduct background verification checks on all candidates for employment, current employees, contractors, and third-party users in accordance with relevant laws and regulations, Buyer's classification of the information to be accessed, and the perceived risks.

4.2.2 A formal disciplinary process shall be established and implemented for employees, contractors, and third-party users who have violated security policies and procedures.

4.3 Supplier shall ensure that all employees, contractors, and third-party users receive appropriate awareness training upon hire and no less than annually thereafter, as well as receive regular updates in Supplier's policies and procedures as relevant to their job function.

5 Risk Management

5.1 Supplier shall create and implement a comprehensive program that manages and mitigates the risk to its information system operations, assets, and Buyer's information.

5.2 Supplier shall perform risk assessments to identify information security risks. Risk assessments are to be performed no less than annually or when major changes occur in the environment, and the results shall be reviewed no less than annually.

6 Organization of Information Security

6.1 Supplier shall ensure that all Supplier Personnel who access Buyer's data will sign confidentiality or non-disclosure documents with Supplier that comply with the applicable legal and security requirements outlined in the Agreement.

6.2 Supplier shall review its approach to managing information security, controls, policies, processes, and procedures as needed, but no less than annually.

6.3 Supplier shall adopt and follow an industry recognized cybersecurity framework such as Health Information Trust Alliance ("HITRUST") framework, National Institute of Standards and Technology (NIST), or International Organization for Standardization (ISO) 27001, unless Buyer otherwise agrees in writing.

6.4 Supplier shall identify the risks to its information and information assets, including from business processes involving third parties, and implement appropriate security controls. Supplier shall evaluate any information security risks posed by third parties prior to establishing a relationship with such third party. Once a relationship has been established, Supplier shall evaluate the third party's information systems on a scheduled ongoing basis.

6.4.1 Supplier shall maintain agreements with its third parties that cover all relevant information security requirements, including as set forth in the Agreements, to the extent that the third parties are accessing, processing, or storing Buyer's data.

6.5 Supplier shall perform risk assessments on its third parties that access, process, and/or store Buyer's data. Supplier agrees to provide evidence of a security assessment of any third parties that have access to Buyer's data.

7 Compliance

7.1 Supplier shall explicitly define, document, and maintain all relevant statutory, regulatory, and contractual requirements for each information system type. Supplier shall similarly define and document the specific controls and individual responsibilities and then communicate them to the user community through a documented security training and awareness program.

7.2 Supplier shall protect all data, documents, information, and records from theft, or loss, or unauthorized or unlawful use, disclosure, modification, alteration, destruction, and falsification in accordance with statutory, regulatory, contractual, and business requirements.

7.3 Supplier shall use cryptographic controls in compliance with all relevant agreements, laws, and regulations. Supplier shall implement strong cryptographic controls for secure file transfers, data at rest and email communications which may contain sensitive information. Supplier's compliance with all relevant regulations shall be reviewed at least on an annual basis.

7.4 Supplier shall develop and maintain audit requirements and activities involving checks on operational systems to minimize the risk of disruptions to business processes. Such audit planning and scoping process shall consider risk, involvement of technical and business staff, other ongoing projects, and business impacts that may impact the effectiveness of the audit.

7.5 Payment Card Industry Information Security Standard Requirements. To the extent Supplier receives, accesses, or transmits cardholder data (e.g., credit or debit card data), Supplier acknowledges its responsibility to secure cardholder data and agrees to comply with applicable Payment Card Industry ("PCI") Data Security Standard ("DSS") requirements.

8 Asset Management

8.1 Supplier shall identify and create an inventory of information assets. All information systems shall be documented and include rules for acceptable use and a method to accurately identify and assign ownership responsibilities to the appropriate users. The rules for acceptable use shall be communicated to all information system users and describe their responsibilities and expected behaviors about information and information system usage.

8.2 Supplier shall classify information based on its value, relevant legal requirements, sensitivity, and criticality to Supplier.

8.2.1 Supplier shall develop and implement an appropriate set of procedures for information labeling and handling in accordance with the classification guidelines adopted by the Supplier. Sensitive information shall be physically and/or electronically labeled and handled appropriately regarding the level of risk the information or document contains.

9 Physical and Environmental Security

9.1 Supplier shall protect secure areas with appropriate physical entry controls to ensure only authorized Supplier Personnel are allowed access. Supplier shall maintain visitor access logs for facilities where information systems reside.

9.2 Supplier shall design and apply physical protections and guidelines for working in secure areas. The arrangements for working in secure areas shall include physical access controls for the Suppliers Personnel and third-party users.

- 9.3 Supplier shall design and implement physical security controls for offices, rooms, and facilities to restrict access from the public.
- 9.4 Supplier shall ensure all items of equipment containing storage media that contain Buyer's data and licensed software have been removed or securely overwritten prior to disposal. Devices containing Buyer's data shall be physically destroyed or the information shall be destroyed, deleted, and overwritten using techniques to make the original information non-retrievable.

10 Communications and Operations Management

- 10.1 Supplier shall formally document and maintain operating procedures for systems associated with information and communication assets and make them available to users on an as-needed basis.
- 10.2 Supplier shall control and archive changes to information assets, systems, networks, and network services. Formal change management responsibilities and procedures shall be in place to ensure satisfactory control of all changes.
- 10.3 Supplier shall establish acceptance criteria for new information systems and any upgrades or new versions of such systems. Supplier shall carry out suitable tests of the systems during development and prior to acceptance to maintain security.
- 10.4 Supplier shall enforce the separation of duties to reduce opportunities for unauthorized or unintentional modification or for misuse of Supplier's assets. No single user shall be able to access, modify or use assets without authorization or detection. Supplier shall identify duties that require separation and define information system access authorizations to support separation of duties.
- 10.5 Supplier shall separate and control development, test, and operational environments to reduce the risks of unauthorized access or changes to the operational system.
- 10.6 Supplier shall implement detection, prevention, and recovery controls to protect against malicious and unauthorized code. Supplier shall maintain a formal enterprise IT security policy and user awareness and compliance program. Supplier shall install updates to its anti-virus or anti-spyware software when available. Supplier shall implement and maintain endpoint security controls, firewalls, and data loss prevention solutions to the most current version available. Supplier shall perform periodic reviews on installed software and the data content of systems to identify and, where possible, remove any unauthorized software, malicious code, or viruses.
- 10.7 Supplier shall create and regularly test back-up copies of information and software and store them in a physically secure remote location at a sufficient distance to make them reasonably immune from damage to data at the primary site. Supplier shall formally document backup processes for systems that process and/or store Buyer's data, which shall include the scope of data being imaged, frequency of imaging, and duration of retention.
- 10.8 Supplier shall manage and control networks to protect Buyer data from anticipated threats or and to maintain the security and integrity of the network, including information in transit. Supplier shall implement controls to ensure the security of information in networks and the protection of connected services from unauthorized access and to ensure the availability of network services and information services using the network. Responsibilities and procedures shall be established for the management of equipment on the network.
- 10.9 Supplier shall document and implement formal procedures for the management of removable media. Media containing Buyer's data shall be physically stored, and its data shall be encrypted in accordance with the Supplier's information security policy on the use of cryptographic controls until the media is destroyed or sanitized in accordance with the confidentiality and integrity requirements for its data classification level.
 - 10.9.1 Supplier shall protect media containing Buyer information against unauthorized access, misuse, or corruption during transportation beyond Supplier's physical boundaries.
- 10.10 Supplier shall establish and implement agreements that specify the minimum set of controls on responsibility, procedures, technical standards, and solutions for the exchange of information and software between Supplier and its third parties.

- 10.11 Supplier shall produce audit logs which record user activities and information security events and Supplier shall maintain such audit logs to assist in future investigations and access control monitoring. Retention for audit logs shall be specified by Supplier and retained accordingly.
- 10.12 Supplier shall protect logging systems and log information against tampering and unauthorized access.
- 10.13 Supplier shall establish procedures for monitoring use of information processing systems and facilities to check for use and effectiveness of implemented controls. The results of the monitoring activities shall be reviewed periodically. Supplier shall comply with all relevant legal requirements applicable to its monitoring activities. Items that shall be monitored include authorized access and unauthorized access attempts.

11 Information Systems Acquisition, Development, and Maintenance

- 11.1 Supplier shall implement verification procedures for the input of business transactions, standing data, parameter tables, and Buyer's data into applications and databases when system development is being performed to ensure that data is correct and appropriate.
- 11.2 Supplier shall validate application data outputs to ensure that the processing of stored information is correct and appropriate to the circumstances. Supplier shall perform output validation manually or automatically when system development on applications and database is being conducted.
- 11.3 Supplier shall develop and implement a policy on the use of cryptographic controls and support it with formal procedures. The cryptographic controls policy shall be aligned with the Supplier's information security policy and shall address the use of encryption for protection of Buyer's data transported by removable media devices or across communication lines.
- 11.4 Supplier shall support the use of cryptographic controls with the practice of key management as set forth in Supplier's cryptographic controls policy. Supplier shall protect all cryptographic keys against modification, loss, and destruction. Supplier shall require protection of secret and private keys against unauthorized disclosure, and all cryptographic keys shall be limited to the fewest number of custodians necessary. Supplier shall physically protect equipment used to generate, store and archive keys, and store encryption keys separately from encrypted data.
- 11.5 Supplier shall carefully select, protect, and control test data in non-production environments. The use of operational databases containing Buyer's data for non-production purposes shall be avoided. If Buyer's data must be used for testing purposes, all sensitive information and content shall be removed or modified beyond recognition before use.
- 11.6 Supplier shall restrict access to program source code and associated items to prevent the introduction of unauthorized functionality and avoid unintentional changes.
- 11.7 Supplier shall supervise and monitor outsourced software development. Supplier shall have a contract for the outsourced development in place with the third party which shall address licensing arrangements, certification of the quality and accuracy of the work carried out, warranties to prevent the transfer of malicious code or viruses, rights of access for audit of the quality and security functionality of code, and escrow arrangements in the event of failure of the third party.
- 11.8 Supplier shall perform penetration testing and vulnerability scans at intervals consistent to industry best practices to identify potential technical vulnerabilities based on notification of zero (0) day vulnerabilities. Supplier shall subscribe to industry recognized threat monitoring service. Once a potential technical vulnerability has been identified, Supplier shall identify the associated risks and the actions to be taken. Such action shall involve patching of vulnerable systems and/or applying other controls. Upon request Supplier shall provide an executive summary report to Buyer of the results of the scans and tests along with a mitigation plan.

12 Information Security Incident Management

- 12.1 Supplier shall report information security incidents to Buyer pursuant to the Agreement. Supplier shall make all employees, contractors and third-party users aware of their responsibility to report any

information security incidents. Supplier shall have documented incident reporting standards and process for employees, contractors and third-party users to report security incidents for further handling.

- 12.2 Supplier shall implement and maintain an incident response plan containing milestones and criteria for its incident response capability, describing the structure and organization of the incident response capability, providing a high-level approach for how the incident response capability aligns with its overall organizational policies and procedures and meets the unique requirements of the Supplier, which relate to mission, size, structure and functions. The incident response plan will also define reportable incidents and resources needed to effectively maintain and mature an incident response capability, as well as provide metrics for measuring the incident response capability. The plan shall then be approved by designated Supplier officials. Formal information security incident reporting procedures to support Supplier's corporate policy shall be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security incident, treating the information security incident as discovered, and the timelines of reporting and response.

12.2.1 Supplier shall review the incident response plan no less than annually and include a table-top exercise, documentation, test plan and results.

12.2.2 Supplier shall make revisions to the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

- 12.3 Supplier shall collect, retain, and present evidence after an information security incident. The evidence that is collected, retained, and presented shall be done in accordance with the laws of the relevant jurisdiction(s).

13 Disaster Recovery Plan and Business Continuity Management

- 13.1 Supplier shall develop and maintain a managed program and process to maintain or restore operations and ensure availability of information at the required level and in the required time frames following interruption to, or failure of, critical business processes for business continuity. Supplier shall maintain a single framework of business continuity plans to ensure all plans are consistent, to address information security requirements, and to identify priorities for testing and maintenance. The program and process shall identify all the assets involved in critical business practices, consider the purchase of suitable insurance, ensure the safety of personnel and the protection of information assets, formulate and document business continuity plans, and address information security requirements in line with the agreed upon business continuity strategy. Supplier shall conduct and review all business continuity planning exercises with all downstream suppliers.
- 13.2 Supplier shall test and annually review business continuity plans to ensure that they are up to date and effective. The business continuity plan tests shall ensure that all members of the recovery team and other relevant staff are aware of their responsibilities for business continuity and information security.

14 Cloud Security

- 14.1 This section is applicable only if the Supplier leverages cloud technologies to perform services for or accesses information belonging to the Buyer.
- 14.2 Supplier shall establish a data protection agreement with its third-party service providers, such as cloud service providers, where Buyer data will be processed or stored.
- 14.3 Supplier shall monitor, review, and perform a security assessment on their cloud service provider(s) that process and store any Buyer data. Upon request, Supplier shall provide Buyer with a copy of the assessment results.
- 14.4 Supplier shall maintain a complete inventory of cloud-based applications and systems in which Buyer data will be processed or stored.
- 14.5 Supplier shall ensure cloud service providers and any cloud-based solutions that are being utilized to deliver the services to the Buyer undergo a security assessment conducted by an independent third-party assessor to assess the security controls not less than annually.

- 14.6 Supplier shall ensure access management controls are implemented in cloud-based environments and applications that will be utilized to process and store any of the Buyer's data. Access management controls shall include but are not limited to implementing multifactor authentication ("MFA"), performing periodic access reviews and ensuring minimum necessary access is granted to systems and applications in which Buyer data will be processed and stored.
- 14.6.1 If security responsibilities for cloud environments are shared between Supplier and Buyer, roles and responsibilities must be documented and communicated. Supplier must notify Buyer promptly of any personnel changes impacting such security responsibilities and operation for the cloud environment.
- 14.7 Supplier shall ensure Buyer data that will be stored in cloud-based applications and systems will be stored and transmitted utilizing industry standard level encryption algorithms such as AES-256. Supplier shall establish an encryption key management policy and procedure for data stored in the cloud environment.
- 14.8 Supplier shall ensure security event log and monitoring alerts are implemented in cloud-based applications and systems in which Buyer data will be processed and stored. System and event logs are retained for a minimum period of one (1) year for cloud environments.
- 14.9 Supplier shall ensure Buyer's data is segregated in cloud-based systems and applications where technically feasible.
- 14.10 Supplier shall ensure cloud service provider stores Buyer's data within the U.S. jurisdiction and geographically distributed locations for primary and redundant data centers.
- 14.11 Supplier shall ensure cloud-service provider follows data retention requirements based on compliance and regulatory requirements.
- 14.12 Supplier shall ensure that the cloud-service provider has a business continuity and disaster recovery plan in place for the cloud environment. Supplier shall ensure business continuity and disaster recovery plans are periodically tested to ensure plans are operating effectively.
- 14.13 Supplier shall ensure cloud service provider maintains an incident response plan and processes for incident escalation and reporting of information security incidents to Supplier. Supplier shall follow Section 12 (Information Security Incident Management) of this document to review and address the information security incident reported by the cloud service provider appropriately.

Supplier agrees to comply with the above Information Security Requirements in form and substance.

By: _____

Name: _____

Title: _____

Date: _____

EXHIBIT 5
SUPPLIER SOFTWARE LICENSE
To be Added or Intentionally Omitted

EXHIBIT 6
OFFSHORE LOCATIONS FORM

Table to be completed by Supplier. Buyer approves of the use of the following offshore locations for Supplier Services or Supplier Personnel identified in the SOW (complete each column for each offshore location):

Line #	Name of entity supplying offshore services Subsidiary/Affiliate name or independent Subcontractor	Specific offshore location address	General description of services	Will offshore location have access to PHI/PII	Will offshore location be receiving and/or storing PHI/PII?	Method of access (VDI, VPN, email, excel, secure file transfer, etc.) / Receipt of PHI/PII may include:	Date location added
1							
2							
3							
4							
5							

If any offshore Services or Supplier Personnel use remote locations other than listed above, Supplier must provide the address of such remote location.