PERFORMANCE WORK STATEMENT (PWS)
For
DGMC 60 MDTS/SGQC
AUTOMATED IMMUNOHEMATOLOGY (BLOOD BANK) ANALYZER
RENTAL/REAGENT SERVICES
5 July 2022

Part 1

General Information

1. GENERAL**:** This is a non-personnel services contract to support David Grant Medical Center's (DGMC) Transfusion Services department (Blood Bank). The Government shall not exercise any supervision or control over the contract service providers performing the services herein. Such contract service providers shall be accountable solely to the Contractor who, in turn is responsible to the Government.

1.1 Description of Services/Introduction: The contractor shall provide all personnel, training, management, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform Immunohematology (Blood Bank) Analyzer Rental/Reagent Services. The Government shall not exercise any supervision or control over the contract service providers performing the services herein. Contract service providers shall be accountable solely to the Contractor who, in turn, is responsible to the Government. The contractor shall provide all personnel, equipment, supplies, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform Cell Saver services as defined in this Performance Work Statement except for those items specified as government furnished property and services. The contractor shall perform to the standards in this contract.

1.2 Background: The Transfusion Services department at David Grant Medical Center is the only Air Force blood bank in California supporting 276K eligible beneficiaries, 2.6K surgeries, and 3K transfusions per year. The Transfusion Services department is accredited by the Food and Drug Administration and the Association of the Advancement of Blood and Biotherapies to perform 75K routine and emergency laboratory testing of patient samples and maintain an inventory of 3K blood products annually.

1.3 Objectives: To provide the blood bank, at David Grant Medical Center (DGMC), with all management, tools, parts, materials, equipment, travel, and labor necessary for rental of Blood Bank Analyzer and reagents by providing an FDA approved analyzer

1.4 Scope: Contractor to provide, safe, dependable, and reliable analyzers to be operated by government personnel assigned to the 60 MDG, David Grant Medical Center at Travis AFB, California.

1.4.1. Contractor shall provide equipment, supplies, and reagents to allow for all test types for workload estimates as identified Technical Exhibit 3, Estimated Workload Data, which have been approved by the U.S. Food & Drug Administration (FDA).

1.4.2. 510(K) of the Food, Drug and Cosmetic Act requires Immunohematology (Blood Bank) Analyzer manufactures to register with the FDA at least 90 days in advance of their intent to market a medical device. This is known as the Premarket Notification- also called PMN or 510(k). Contractor must be in compliance with Section 510(K) of the Federal Food, Drug and Cosmetic Act for those medical device products intended to be delivered to the Government. Only devices that have received Premarket Notification Approval from the FDA will be authorized under contract and installed at the MTF.

1.4.3. Contractor shall be available for service assistance and onsite repair or assistance when required. Response time: phone within 4 hours; On-site within 48 hours; 24 hours online technical support. For repair, the contractor shall make telephone contact to the Quality Assurance Personnel (QAP) within 4 hours and be on-site within 48 hours after notification. In addition, repair technicians must be certified by the OEM to perform all necessary maintenance and or repair. All parts and supplies must be manufactured and certified by the OEM as well as carry the equivalent warranties.

1.4.4. The device and all associated components must be included in the Authorization to Operate (ATO) accreditation boundary. The analyzer and all associated components must meet all DoD Cyber Security Measures with an Authorization to Operate (ATO) and be compatible for Bi-Directional Interface with Military Health System (MHS) Genesis connectivity and the Laboratory Information System (LIS). The Government shall not exercise any supervision or control over the contract service providers performing the services herein. Such contract service providers shall be accountable solely to the Contractor who, in turn is responsible to the Government.

1.4.5. Properly maintain and dispose of records.

1.4.6. Service Reporting of all service calls for equipment maintenance must be reported to the laboratory and to the Medical Equipment Repair Center (MERC) located at the MTF. Reports will be signed off by the laboratory personnel, to include date, time, company name and service representative, contract number, description of malfunction, description of any services performed, and any recommendations necessary to maintain equipment in the best operating condition. Documentation, verifying repair technicians are OEM certified and that only OEM parts will be used and must be provided to the contracting officer within 30 days of award. All services must be performed according to OEM procedures and be guaranteed to the same extent as provided by the OEM.

1.5. Period of Performance: The period of performance shall be for one (1) base year and two (two) option 12-month option years.

Base Year: 1 April 2023 – 31 March 2024
Option Year I: 1 April 2024 – 31 March 2025
Option Year II: 1 April 2025 – 31 March 2026

1.6 General Information

1.7 Quality Control: The contractor shall develop and maintain an effective Quality Control (QC) program to ensure services are performed in accordance with this PWS. The contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The contractor's QC program is the means by which to confirm work complies with the requirement of the contract with the contractor's proposal. After acceptance of the quality control plan the contractor shall receive the contracting officer's acceptance in writing of any proposed change to the QC system.

1.8 Quality Assurance: The government shall evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan. This plan is primarily focused on what the Government must do to ensure that the contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

1.9 Recognized Holidays: Contractor is required to provide services on all federal holidays. Holidays recognized:

New Year's Day
Martin Luther King Jr.'s Birthday
President's Day
Memorial Day
Juneteenth
Independence Day
Labor Day
Columbus Day
Veteran's Day
Thanksgiving Day
Christmas Day

1.10 Hours of Operation: The Transfusion Services department is a 24/7 operation. The contractor is responsible for providing services during hours of operation and as outlined by section 1.4.3 of this PWS for equipment maintenance. The contractor is responsible for conducting business between the hours of 7:30 am – 4:30 pm Pacific Time, Monday through Friday, except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor must always maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. When hiring personnel, the Contractor shall keep in mind that the stability and continuity of the workforce are essential.

1.11 Place of Performance: The work to be performed under this contract will be performed at David Grant Medical Center, Travis Air Force Base, California.

1.12 Type of Contract: The government will award a Firm Fixed Price Contract.

1.13 Security Requirements: The MTF will conduct criminal history background checks (CHBC) on all HCWs involved in the delivery of healthcare to children, under the age of 18 on a frequent and regular basis, as stated in the DoDI 1402.5, The Contractor is responsible for ensuring the HCW completes additional local forms when meeting with the Unit Security Manager. Checks will be process IAW MDGI 44-39, Background Investigation of Persons Providing Care to Children and AFI 44-119, para 5.4.7. Staff may be employed under the contract pending completion of the background checks but will require "close clinical supervision" as outlined in AFI 44-119, paragraph 5.4.7. The MTF Commander will determine if a HCW will be able to work pending a CHBC and make the decision on quality assurance, risk management, licensure, employee orientation, and credentials verification. Close clinical supervision for HCWs who's CHBCs are pending may include supervised privileges or line of site supervision (i.e., chaperoned by an individual whose background check has been successfully completed) to ensure the protection of patients under the age of 18.

1.14 PHYSICAL Security: The contractor shall be responsible for safeguarding all government equipment, information and property provided for contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

1.15. Contractor Identification: All contractor management staff, or contracted employee shall clearly be identified as such at all times, including conversations, mail, email, faxes, and/or other electronic communication whether with government personnel, other contractor personnel, or with public when supporting this contract. Likewise, the contractor shall abide by all applicable laws and regulations when using government equipment and services in performance of this contract. As a minimum, contractor management staff or contracted personnel shall clearly identify themselves as contractors by wearing badges which clearly and legibly identify the employee as a contractor, using the label "contractor" in email addresses in accordance with Federal Acquisition Regulation (FAR) 37.114. MTF issued identification badge shall be worn above the waistline during the individual's duty hours.

1.16. Post Award Conference/Periodic Progress Meetings: The Contractor agrees to attend any post award conference convened by the contracting activity or contract administration office in accordance with Federal Acquisition Regulation Subpart 42.5. The contracting officer, Contracting Officers Representative (COR), and other Government personnel, as appropriate, may meet periodically with the contractor to review the contractor's performance. At these meetings the contracting officer will apprise the contractor of how the government views the contractor's performance and the contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the government.

1.17. Contracting Officer Representative (COR): The (COR) will be identified by separate letter. The COR monitors all technical aspects of the contract and assists in contract administration The COR is authorized to perform the following functions: assure that the Contractor performs the technical requirements of the contract: perform inspections necessary in connection with contract performance: maintain written and oral communications with the Contractor concerning technical aspects of the contract: issue written interpretations of technical requirements, including Government drawings, designs, specifications: monitor Contractor's performance and notifies both the Contracting Officer and Contractor of any deficiencies; coordinate availability of government furnished property, and provide site entry of Contractor personnel. A letter of designation issued to the COR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the COR, especially about changes in cost or price, estimates or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting order.

1.18. Key Personnel: The following personnel are considered key personnel by the government: COR and KO. The contractor shall provide a contract manager who shall be responsible for the performance of the work. The name of this person and an alternate who shall act for the contractor when the manager is absent shall be designated in writing to the contracting officer. The contract manager or alternate shall have full authority to act for the contractor on all contract matters relating to daily operation of this contract. The contract manager or alternate shall be available between 7:30 a.m. to 4:30

p.m. Pacific Time, Monday thru Friday except Federal holidays or when the government facility is closed for administrative reasons.

1.19. Identification of Contractor Employees: IAW DFARS Subpart 211.106 Service contracts shall require contractor employees to identify themselves as contractor personnel by introducing themselves or being introduced as contractor personnel and displaying distinguishing badges or other visible identification for meetings with Government personnel. In addition, contracts shall require contractor personnel to appropriately identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence. They must also ensure that all documents or reports produced by are suitably marked as contractor products or that participation is appropriately disclosed. Contractor personnel will be required to obtain and wear visitor badges in the performance of this service.

1.20. Contractor Travel: N/A

1.21. Other Direct Costs: N/A

1.22. Data Rights: The Government has unlimited rights to all documents/material produced under this contract. All documents and materials, to include the source codes of any software, produced under this contract shall be Government owned and are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the contractor without written permission from the Contracting Officer. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

1.23. Organizational Conflict of Interest: Contractor and subcontractor personnel performing work under this contract may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications, or work statements, etc.) or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

1.24. Phase In /Phase out Period: To minimize any decreases in productivity and to prevent possible negative impacts on additional services, the Contractor shall have personnel on board, during the 30-day phase in/ phase out periods. During the phase in period, the Contractor shall become familiar with performance requirements to commence full performance of services on the contract start date.

1.25 Contractor Reporting Requirement: Contractor will report manpower data relating to the performance of services contracts to the COR on a weekly basis.

PART 2
DEFINITIONS & ACRONYMS

2. **DEFINITIONS AND ACRONYMS:**

2.1. DEFINITIONS:

2.1.1. AUTHORIZATION TO OPERATE (ATO). An Authorization to Operate (ATO) is a formal declaration by a Designated Approving Authority (DAA) that authorizes operation of a Business Product and explicitly accepts the risk to agency operations. The ATO is signed after a Certification Agent (CA) certifies that the system has met and passed all requirements to become operational.

2.1.1. CONTRACTOR. A supplier or vendor awarded a contract to provide specific supplies or service to the government. The term used in this contract refers to the prime.

2.1.2. CONTRACTING OFFICER. A person with authority to enter into, administer, and or terminate contracts, and make related determinations and findings on behalf of the government. Note: The only individual who can legally bind the government.

2.1.3. CONTRACTING OFFICER'S REPRESENTATIVE (COR). An employee of the U.S. Government appointed by the contracting officer to administer the contract. Such appointment shall be in writing and shall state the scope of authority and limitations. This individual has authority to provide technical direction to the Contractor as long as that direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have authority to change the terms and conditions of the contract.

2.1.4. DEFECTIVE SERVICE. A service output that does not meet the standard of performance associated with the Performance Work Statement.

2.1.5. DELIVERABLE. Anything that can be physically delivered but may include non-manufactured things such as meeting minutes or reports.

2.1.6. KEY PERSONNEL. Contractor personnel that are evaluated in a source selection process and that may be required to be used in the performance of a contract by the Key Personnel listed in the PWS. When key personnel are used as an evaluation factor in best value procurement, an offer can be rejected if it does not have a firm commitment from the persons that are listed in the proposal.

2.1.7. PHYSICAL SECURITY. Actions that prevent the loss or damage of Government property.

2.1.8. QUALITY ASSURANCE. The government procedures to verify that services being performed by the Contractor are performed according to acceptable standards.

2.1.9. QUALITY ASSURANCE Surveillance Plan (QASP). An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance.

2.1.10. QUALITY CONTROL. All necessary measures taken by the Contractor to assure that the quality of an end product or service shall meet contract requirements.

2.1.11. SUBCONTRACTOR. One that enters into a contract with a prime contractor. The Government does not have private of contract with the subcontractor.

2.1.12. WORKDAY. The number of hours per day the Contractor provides services in accordance with the contract.

2.1.12. WORK WEEK. Monday through Friday, unless specified otherwise.

2.2. ACRONYMS:

AABB	Association for Advancement of Blood and Biotherapies
ATO	Authority to Operate
CCE	Contracting Center of Excellence
CFR	Code of Federal Regulations

CONUS	Continental United States (excludes Alaska and Hawaii)
COR	Contracting Officer Representative
COTR	Contracting Officer's Technical Representative
COTS	Commercial-Off-the-Shelf
DA	Department of the Army
DD250	Department of Defense Form 250 (Receiving Report)
DD254	Department of Defense Contract Security Requirement List
DFARS	Defense Federal Acquisition Regulation Supplement
DMDC	Defense Manpower Data Center
DOD	Department of Defense
FAR	Federal Acquisition Regulation
HIPAA	Health Insurance Portability and Accountability Act of 1996
KO	Contracting Officer
OCI	Organizational Conflict of Interest
OCONUS	Outside Continental United States (includes Alaska and Hawaii)
ODC	Other Direct Costs
PIPO	Phase In/Phase Out
POC	Point of Contact
PRS	Performance Requirements Summary
PWS	Performance Work Statement
QA	Quality Assurance
QAP	Quality Assurance Program
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Program
TE	Technical Exhibit

PART 3
GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

3. GOVERNMENT FURNISHED ITEMS AND SERVICES:

3.1 Facilities: The Government will provide required limited space for delivery and installation of equipment.

3.2 Utilities: The Government will provide limited laboratory floor space for installation of equipment, to include electrical, water, sewage as necessary for the functionality of equipment The Contractor shall instruct employees in utilities conservation practices. The contractor shall be responsible for operating under conditions that preclude the waste of utilities, which include turning off the water faucets or valves after using the required amount to accomplish cleaning vehicles and equipment.

PART 4
CONTRACTOR FURNISHED ITEMS AND SERVICES

4. CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES:

4.1 General: The Contractor shall furnish all manpower, shipping, installation, supplies, equipment, services, and training required to perform work under this contract that are not listed under Part 5 and Technical Exhibit 1.

4.3. Materials: The Contractor shall, furnish all tools and materials, reagents/supplies, and equipment necessary to meet the requirements under this PWS.

4.4. Equipment: The Contractor shall provide all equipment and service maintenance required to meet technical requirements as outlined in Part &, Technical Exhibit.

PART 5
SPECIFIC TASKS

5. Specific Tasks:

5.1. Basic Services. The contractor shall provide equipment and services for automated Immunohematology (Blood Bank) testing capabilities.

5.2. Task Heading.

5.2.1. Contractor to provide, safe, dependable, and reliable analyzers to be operated by government personnel assigned to the 60 MDG, David Grant Medical Center at Travis AFB, California.

5.2.2. Contractor shall provide equipment, supplies, and reagents to allow of all the test types for workload estimates as identified Technical Exhibit 1, which have been approved by the U.S. Food & Drug Administration (FDA). 510(K) of the Food, Drug and Cosmetic Act requires Immunohematology (Blood Bank) Analyzer manufactures to register with the FDA at least 90 days in advance of their intent to market a medical device. This is known as the Premarket Notification- also called PMN or 510(k). Contractor must be in compliance with Section 510(K) of the Federal Food, Drug and Cosmetic Act for those medical device products intended to be delivered to the Government. Only devices that have received Premarket Notification Approval from the FDA will be authorized under contract and installed at the MTF.

5.2.3. Contractor shall be available for service assistance and onsite repair or assistance when required. Response time: phone within 4 hours; On-site within 48 hours; 24 hours online technical support. For repair, the contractor shall make telephone contact to the Quality Assurance Personnel (QAP) within 4 hours and be on-site within 48 hours after notification. In addition, repair technicians must be certified by the OEM to perform all necessary maintenance and or repair. All parts and supplies must be manufactured and certified by the OEM as well as carry the equivalent warranties.

5.2.4. The device and all associated components must be included in the Authorization to Operate (ATO) accreditation boundary. The analyzer and all associated components must meet all DoD Cyber Security Measures with an Authorization to Operate (ATO) and be compatible for Bi-Directional Interface with Military Health System (MHS) Genesis connectivity and the Laboratory Information System (LIS). The Government shall not exercise any supervision or control over the contract service providers performing the services herein. Such contract service providers shall be accountable solely to the Contractor who, in turn is responsible to the Government.

5.2.5. Properly maintain and dispose of records.

5.2.6. Service Reporting of all service calls for equipment maintenance must be reported to the laboratory and to the Medical Equipment Repair Center (MERC) located at the MTF. Reports will be signed off by the laboratory personnel, to include date, time, company name and service representative, contract number, description of malfunction, description of any services performed, and any recommendations necessary to maintain equipment in the best operating condition. Documentation, verifying repair technicians are OEM certified and that only OEM parts will be used and must be provided to the contracting officer within 30 days of award. All services must be performed according to OEM procedures and be guaranteed to the same extent as provided by the OEM.

PART 6
APPLICABLE PUBLICATIONS

6. **APPLICABLE PUBLICATIONS (CURRENT EDITIONS)**:

6.1. The Contractor must abide by all applicable regulations, publications, manuals, and local policies and procedures.

6.1.1. Code of Federal Regulations Title 21, Part 640

6.1.2. AFMAN 41-111, Standards for Blood Banks and Transfusion Services, Current Edition

PART 7
ATTACHMENT/TECHNICAL EXHIBIT LISTING

7. Attachment/Technical Exhibit List:

7.1. Attachment 1/Technical Exhibit 1 – Performance Requirements Summary

7.2. Attachment 2/Technical Exhibit 2 – Deliverables Schedule

7.3 Attachment 3/Technical Exhibit 3 – Estimated Workload Data

TECHNICAL EXHIBIT 1

Performance Requirements Summary

The contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success.

Performance Objectives	**Performance Threshold**	**Method of Surveillance**	**Procedure**
Safe, dependable, and reliable operation of Blood Bank Analyzer equipment according to published operating specifications	100 % Compliance	Operational up-time 95% or higher	The QAP will prepare a monthly report to ensure products and services are within stated performance thresholds.
The contractor will maintain required certification with the FDA	100 % Compliance	Certification must be current through the life of the contract	The QAP will prepare an annual report utilizing accreditation certificates to ensure products and services are within stated performance thresholds.
Response time: phone contact within 4 hours. On-site within 48 hours. Online technical support for capable equipment.	100 % Compliance	Review of data; periodic inspection of the contractor's job performance during the duration of this contract; customer feedback, timeliness, legibility, and accuracy.	The QAP will monitor response time and prepare a monthly report to ensure stated performance thresholds are met.
Delivery Performance	100 % Compliance	Review of data; periodic inspection of the contractor's job performance during the duration of this contract; customer feedback, timeliness, legibility, and accuracy.	The QAP will prepare a monthly report to ensure products and services are within stated performance thresholds.
Cyber Security	Meet DoD Cyber Security	Review of data; periodic inspection of the contractor's job performance during the duration of this contract; customer feedback, timeliness,	The QAP will monitor the requirement and prepare a monthly report to ensure stated performance thresholds are met.

		legibility, and accuracy.	
Defense Health Agency Authorization to Operate (ATO)	The device and all associated components must be included in the Authorization to Operate (ATO) accreditation boundary.	Review of data; periodic inspection of the contractor's job performance during the duration of this contract; customer feedback, timeliness, legibility, and accuracy.	The QAP will monitor the requirement and prepare a monthly report to ensure stated performance thresholds are met.
Bi-Directional Interface with Military Health System (MHS) Genesis connectivity and the laboratory information system (LIS)	a) The system shall have the ability to receive HL7 order messages (ORM) and information from the LIS and provide DICOM Modality Worklist to the modalities. b) If the vendor is not already approved to connect to Military Health System (MHS) Genesis bi-directionally, the vendor shall agree to complete any bi-directional interface integration at no additional cost to the Government. Interface integration must be completed prior to final acceptance of the system.	Review of data; periodic inspection of the contractor's job performance during the duration of this contract; customer feedback, timeliness, legibility, and accuracy.	The QAP will monitor the requirement and prepare a monthly report to ensure stated performance thresholds are met.

Performance Item	Our Requirements
Model type	Benchtop
Technology requirement	Automated Immunohematology Tests
Test types supported	Direct Agglutination Tests, Direct Antiglobulin Tests, and Indirect Antiglobulin Tests
Specific test capability	ABO Forward/Reverse grouping, Rh typing, Rh phenotyping, antigen typing, DAT, IgG DAT, antibody screening, antibody identification, and IAT crossmatching, cord blood testing and serial dilutions for titrations studies.
Analyzer functions	Red cell suspension preparation, sample and reagent dispensing, incubation, centrifugation, reading/interpretation by image analysis
Analyzer software functions	Import work orders from MHS Genesis, positive identification of gel cards, samples, and reagents, create worksheets (grouped tests) to allow continuous operation, verify batch results against the results of Quality Control samples, data storage of test results, result data export to the MHS Genesis. The system shall have the ability to receive HL7 order messages and information from the MHS Genesis provide DICOM Modality Worklist to the modalities.
Analyzer reagents	No manual reconstitution or dilutions

Analyzer security features	Ability to define access privileges by users, user passwords, required periodic modification of user passwords, ability to inactivate users, users cannot readily access the instrument functional and data files on analyzer computer.
Manual tube testing reagents	Must carry full line of FDA approved tube testing reagents to provide secondary back up support for analyzer capabilities.
Contract compliance	This “Cost-Per-Test” priced contract must provide 1 analyzer IAW Appendix II, reagent shipments in accordance with Appendix II to include shipping costs, equipment training and equipment repair and maintenance for the contracted analyzer
Regulatory	
	Instrument and all assays are currently FDA approved (Vendor must provide proof of certification)
	In the past 24 months: No FDA warning letters issued, No FDA required action plan issued, no major FDA non-compliance (483's) issued.
	Establishment Inspection Records (EIR's) available for review
	Meets OSHA requirements
	Underwriters Laboratories certification for electrical safety for laboratory use
	Product recall letters available for past 24 months
	No class 1 or class 2 recalls in the past 3 years
Training	
	Vendor provides a minimum of one factory training slots in first year and one additional slot each option year
	Flexible on-site training program available
Validations	Must provide and perform required Method Conversion (method validation) protocols for each specific test capabilities with onsite staff, documentation, and technical support.
Technical Support	24/7 Telephone Technical Support

TECHNICAL EXHIBIT 2

DELIVERABLES SCHEDULE

Product delivery schedule for supplies required to perform estimated number of tests as outlined in Technical Exhibit II, Estimated Workload

Deliverable	Frequency	# of Copies	Medium/Format	Submit To

Quantity	Product	Ship Dates	Number of Shipment each year	Est Qty each year (Qty X shipments)
5	3% Surgiscreen	Every 28 Days	13	65
5	3% Affirmagen	Every 28 Days	13	65
1	3% Resolve Panel A	Every 28 Days	13	13
3	3% Coombs Control	Every 28 Days	13	39
2	Confidence Kit	Every 28 Days	13	26
1	3% Resolve Panel B	Every 28 Days	13	13
8	0.8% Surgiscreen	Every 28 Days	13	104
8	0.8% Affirmagen	Every 28 Days	13	104
1	0.8% Resolve Panel A	Every 28 Days	13	13
1	0.8% Resolve Panel B	Every 28 Days	13	13
5	AlbaQ-Chek®	Every 28 Days	13	65
1	Round Diluent 2	Every 28 Days	13	13
2	Round Diluent 2+	Every 28 Days	13	26
1	Manual Pipette Tips	Every 28 Days	13	13
4	Anti-IgG Card	Every 28 Days	13	52
7	A/B/D Mono Reverse Card	Every 28 Days	13	91
1	Fetal Screen	Every 28 Days	13	13
1	Complement Control Cells	Every 28 Days	13	13
Quantity	**Product**	**Ship Dates**	**Number of Shipment each year**	**Est Qty each year (Qty X shipments)**
2	Anti-A BioClone	Every 84 Days	4	8
2	Anti-B BioClone	Every 84 Days	4	8
2	Anti-D BioClone	Every 84 Days	4	8
5	Antibody Enhancement	Every 84 Days	4	20
6	Anti-C Bioclone	Every 84 Days	4	24
7	Anti-E Bioclone	Every 84 Days	4	28
6	Anti-c Bioclone	Every 84 Days	4	24
4	Anti-e Bioclone	Every 84 Days	4	16
1	Rh Control	Every 84 Days	4	4
5	Anti-Kell	Every 84 Days	4	20
1	Anti Fya	Every 84 Days	4	4
5	Anti-IgG C3D Cards	Every 84 Days	4	20
6	ABD/ABD Mono Group Card	Every 84 Days	4	24
5	Buffered Gel Card	Every 84 Days	4	20
Quantity	**Product**	**Ship Dates**	**Number of Shipment each year**	**Est Qty each year (Qty X shipments)**
1	Anti-IgG Green	Every 168 Days	2	2
1	Anti-M	Every 168 Days	2	2
1	Anti-S	Every 168 Days	2	2
1	Anti-Fyb	Every 168 Days	2	2
1	Anti-s	Every 168 Days	2	2
4	Anti-Jka BioClone	Every 168 Days	2	8

Deliverable	Frequency	# of Copies	Medium/Format	Submit To
1	Anti-Jkb BioClone	Every 168 Days	2	2
1	Anti-k	Every 168 Days	2	2
Quantity	**Product**	**Ship Dates**	**Number of Shipment each year**	**Est Qty each year (Qty X shipments)**
1	Anti-C3D Monoclonal	Every 365	1	1

TECHNICAL EXHIBIT 3

ESTIMATED WORKLOAD DATA

Item	Name	Estimated Annual Test Volume
1	ABO/Rh	4000
2	ABO/Rh Confirmation	972
3	Weak D Typing	168
4	Antibody Screen	2460
5	Antibody Identification	111
6	DAT	15
7	Antigen Typing	14
8	Crossmatch	927
9	Cord Sample ABO/Rh	293
10	Cord Sample DAT	293

Department of Defense (DOD) Business Associate Agreement (BAA)

Introduction

In accordance with 45 CFR §§164.502(e)(2), 164.504(e); the Health Information Technology for Economic and Clinical Health (HITECH) Act; and paragraph 3.3.c. of Department of Defense Manual (DoDM) 6025.18, "Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs," March 13, 2019, and Chapter 1, Section 5 of the TRICARE Operations Manual, this document serves as a Business Associate Agreement (BAA) between the executing parties for purposes of the Health Insurance Portability and Accountability Act (HIPAA) as implemented by the HIPAA Rules and Department of Defense (DoD) HIPAA Issuances (as defined below). The parties are a DoD Component, acting as a HIPAA Covered Entity, and a Business Associate (i.e., a DoD Contractor creates, receives, maintains, and/or transmits protected health information (PHI) for the purpose of performing covered functions on behalf of the DoD Component). The HIPAA Rules (as defined below) require BAAs between covered entities and business associates. As such, this BAA implements and incorporates the applicable DoD HIPAA Issuances (including DoDI 6025.18 and the authorities incorporated therein) and provides the Business Associate requirements which apply to the relevant Business Associates contract or other agreement between the parties.

(a) **Catchall Definition**: Except as otherwise provided in this BAA, the following terms used in this BAA shall have the same meaning as those terms in the DoD HIPAA Issuances: Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices (NoPP), PHI, Required by Law, Secretary of HHS, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

(b) **Specific definitions**:

Agreement means this BAA together with the documents and/or other arrangements under which the Business Associate signatory performs services involving access to PHI on behalf of the DOD component signatory.

Breach means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: (1) a person other than an authorized user accesses or potentially accesses personally identifiable information; or (2) an authorized user accesses or potentially accesses Personally Identifiable Information (PII) for another than authorized purpose. The foregoing definition is based on the definition of breach in Office of Management and Budget (OMB) Memorandum M-17-12.

Business Associate shall generally have the same meaning as the term "Business Associate" in the DoD HIPAA Issuances, and in reference to this BAA, shall mean *[insert name of the non-federal Business Associate entity/signatory to this BAA]*.

Covered Entity shall generally have the same meaning as the term "covered entity" in the DoD HIPAA Issuances, and in reference to this BAA, shall mean *[insert name of the DOD Component entity/DoD signatory to this BAA].*

Covered Functions are functions of a covered entity, the performance of which makes the entity a health plan or health care provider as outlined in DoDM 6025.18.

Defense Health Agency (DHA) Privacy Office means the DHA Privacy and Civil Liberties Office, with the responsibilities and authorities as outlined in DoDM 6025.18. The Chief of the DHA Privacy Office is the HIPAA Privacy and Security Officer for DHA.

DoD HIPAA Issuances means all DOD issuances implementing the HIPAA Rules in the DoD Military Health System (MHS). These issuances include DoDM 6025.18 (2019), Department of Defense Instruction (DoDI) 6025.18, "Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs,"

March 13, 2019; and DoDI 8580.02, "Security of Individually Identifiable Health Information in DoD Health Care Programs," August 12, 2015.

DoD Privacy Program Issuances means the current DOD issuances implementing within DOD the Privacy Act and certain privacy-related authorities, as identified by DHA Privacy Office Guidance. These issuances are DoDI 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019, DoDM 5400.11, Volume 2 "DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan," May 6, 2021, and DOD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007. These issuances are available on the Washington Headquarters Services DOD Directives website (https://www.esd.whs.mil/DD/) or upon request.

Department of Health and Human Services (HHS) Breach means a breach that satisfies the HIPAA Breach Rule definition of breach found in 45 CFR §164.402.

HIPAA Rules means the regulations issued by HHS pursuant to its authority to issue regulations on health information privacy, as provided by Section 264(c) of HIPAA. The HIPAA Rules, as amended by the Omnibus Final Rule, include the HIPAA Privacy Rule, the HIPAA Breach Rule, the HIPAA Security Rule, and the HIPAA Enforcement Rule.

I. Obligations and Activities of the Business Associate

(a) The Business Associate shall not use or disclose PHI other than as permitted or required by the Agreement or as required by law.

(b) The Business Associate shall use appropriate safeguards and comply with the HIPAA Rules and DoD HIPAA Issuances incorporated by reference in this document Issuances with respect to PHI, to prevent use or disclosure of PHI other than as provided for by the Agreement.

(c) The Business Associate shall report to the Covered Entity any breach of which it becomes aware and shall proceed with breach response steps as required by Part V of this agreement. With respect to electronic PHI, the Business Associate shall also respond to any security incident of which it becomes aware in accordance with any cybersecurity provisions of the Agreement. If at any point the Business Associate becomes aware that a security incident involves a breach, the Business Associate shall immediately initiate breach response as required by PartV of this BAA.

(d) In accordance with DoDM 6025.18, paragraph 3.3.c.(3)(b)4, 45 CFR §164.502(e)(1)(ii)) and §164.308(b)(2),the Business Associate shall ensure that any (and all) subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to PHI, specifically the responsibilities laid out in the DoD HIPAA Issuances incorporated by reference in this agreement. PHI.

(e) The business associate may disclose PHI to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit PHI on its behalf, if the business associate obtains satisfactory assurances, in accordance with DoDM 6025.18, paragraph 4.5.e.(1), that the subcontractor will appropriately safeguard the information.

(f) The Business Associate shall make available PHI in a Designated Record Set, to the Covered Entity or, as directed by the Covered Entity, to an Individual, as necessary to satisfy the Covered Entity obligations under 45 CFR §164.524 and DoDM 6025.18, paragraph 5.3.c.

(g) The Business Associate shall make any amendment(s) to PHI in a Designated Record Set as directed or agreed to by the Covered Entity pursuant to 45 CFR § and DoDM 6025.18, paragraph 5.4.

(h) The Business Associate shall maintain and make available the information required to provide an accounting

of disclosures to the Covered Entity or an individual as necessary to satisfy the Covered Entity's obligations under 45 CFR §164.528 and DoDM 6025.18, paragraph 5.5.

(i) To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under the HIPAA Privacy Rule and DoDM 6025.18, the Business Associate shall comply with the requirements of the HIPAA Privacy Rule and DoDM 6025.18, that apply to the Covered Entity in the performance of such obligation(s); and

(j) The Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI from or created or received by the Business Associate on behalf of, the DOD Component available to the Secretary of HHS and to the Director, DHA, or their designee for purposes of determining compliance with the HIPAA Rules.

II. Permitted Uses and Disclosures by Business Associate

(a) The Business Associate may only use or disclose PHI as necessary to perform the services set forth in the Agreement or as required by law. The Business Associate is not permitted to de-identify PHI, nor is it permitted to use or disclose de-identified PHI, except as provided by the Agreement or directed by the Covered Entity with written approval from DHA's HIPAA Privacy Officer.

(b) The Business Associate agrees to use, disclose, and request PHI only in accordance with the HIPAA Privacy Rule "minimum necessary" standard and corresponding DHA policies and procedures as stated in the DoD HIPAA Issuances.

(c) The Business Associate shall not use or disclose PHI in a manner that would violate the DoD HIPAA Issuances if done by the Covered Entity.

(d) Except as otherwise limited in the Agreement, the Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate. The foregoing authority to use PHI does not apply to disclosure of PHI, which is covered in the next paragraph.

(e) Except as otherwise limited in the Agreement, the Business Associate may disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that disclosures are required by law, or the Business Associate obtains reasonable assurances from the person to whom the PHI is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(f) Except as otherwise limited in the Agreement, the Business Associate may use PHI to provide Data Aggregation services relating to the Covered Entity's health care operations.

III. Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) The Covered Entity shall provide the Business Associate with NoPP that the Covered Entity produces in accordance with 45 CFR §164.520 and DoDM 6025.18, paragraph 5.1.

(b) The Covered Entity shall notify the Business Associate of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes affect the Business Associate's use or disclosure of PHI.

(c) The Covered Entity shall notify the Business Associate of any restriction on the use or disclosure of PHI that

the Covered Entity has agreed to or is required to abide by under 45 CFR §164.522 and DoDM 6025.18, paragraph 5.2, to the extent that such changes may affect the Business Associate's use or disclosure of PHI.

IV. Permissible Requests by Covered Entity

The Covered Entity shall not request the Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule or any applicable Federal regulations (including without limitation, DoD HIPAA Issuances) if done by the Covered Entity.

V. Breach Response

(a) In general.

In the event of a breach of PII/PHI held by the Business Associate, the Business Associate shall follow the breach response requirements set forth in this Part V, which is designed to satisfy both the Privacy Act and HIPAA breach response requirements, as applicable. If a breach involves PII without PHI, then the Business Associate shall comply with DoD Privacy Program Issuances breach response requirements only. If a breach involves PHI (a subset of PII), then the Business Associate shall comply with DoD Privacy Program Issuances breach response requirements. A breach involving PHI may or may not constitute an HHS Breach. If a breach is not an HHS Breach, then the Business Associate has no HIPAA breach response obligations. In such cases, the Business Associate must still comply with breach response requirements under the DoD Privacy Program Issuances.

If the DHA Privacy Office determines that a breach is an HHS Breach, then the Business Associate shall comply with both the HIPAA Breach Rule and DoD Privacy Program Issuances, as directed by the DHA Privacy Office. If the DHA Privacy Office determines that the breach does not constitute an HHS Breach, then the Business Associate shall comply with DoD Privacy Program Issuances. The following provisions of Part V set forth the Business Associate's Privacy Act and HIPAA breach response requirements for all breaches, including but not limited to HHS breaches.

In general, for breach response, the Business Associate shall report the breach to the Covered Entity. Such breach shall be reported to the DHA Privacy Office within 24 hours at 703-275-6363 or dha.privacyofficer@mail.mil. If such breach is a cybersecurity incident, an incident involving damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, electronic communication, including information contained therein, ensuring the availability, integrity, authentication, confidentiality, and nonrepudiation of data, as defined in Committee on National Security Systems Instruction (CNSSI) 4009 https://www.cnss.gov/CNSS/issuances/Instructions.cfm, the discovering party shall report the breach to the DHA NIWC CSSP Watch desk by dialing 1.866.786.4432 Cybersecurity and Infrastructure Security Agency potential-CERT) within one hour of the potential cybersecurity incident. The DHA NIWC CSSP Watch desk reports, and report to USCYBERCOM within 48 hours of being notified of the occurrence of a breach, and complete the breach response actions as required by DHA guidance https://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Breaches-of-PII-and-PHI?type=Policies#RefFeed.

The Business Associate is deemed to have discovered a breach as of the first day a breach (suspected or confirmed) is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing it) who is an employee, officer, or other agent of the Business Associate.

The Business Associate shall submit a report to the U.S. Computer Emergency Readiness Team (US-CERT), using the US-CERT report online form at https://us-cert.cisa.gov/forms/reporthttps://us-cert.cisa.gov/forms/report. Before submission to US-CERT, the Business Associate shall save a copy of the on-line report. After submission, the Business Associate shall record the US-CERT Reporting Number. Although only limited information about the breach may be available as of the one-hour deadline for submission, the Business Associate shall submit the US-CERT report by the deadline. The Business Associate shall e-mail updated information to the Covered Entity as it is obtained. The Business Associate shall provide a copy of the initial or updated US-CERT report to the DHA Privacy Office. Business Associate general questions about US-CERT reporting shall be directed to the DHA Privacy Office not the US-CERT office.

Additionally, the Business Associate will send to the DHA Privacy Office a completed Breach Report Form Report DD 2959 at https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd2959.pdf. Encryption is not required, because Breach Report Forms must not contain PII/PHI.

If multiple individuals are affected by a single event or related set of events, then a single reportable breach may be deemed to have occurred, depending on the circumstances. The Business Associate shall inform the DHA Privacy Office as soon as possible if it believes that a "single event" breach response is appropriate. The DHA Privacy Office will determine how the Business Associate shall proceed and, if appropriate, consolidate separately reported breaches for purposes of Business Associate report updates, individual notification, and mitigation.

When an initially submitted Breach Report Form is incomplete or incorrect due to unavailable information, or when significant developments require an update, the Business Associate shall submit a revised form or forms, stating the updated status and previous report date(s) and showing any revisions or additions by denoting "UPDATE." Examples of updated information the Business Associate shall report include but are not limited to confirmation on the exact data elements involved, the root cause of the incident, and any mitigation actions, including sanctions, training, incident containment, follow-up, etc. The Business Associate shall submit these report updates promptly after the new information becomes available. Prompt reporting of updates is required to allow the DHA Privacy Office to make timely final determinations on any subsequent notifications or reports. The Business Associate shall provide updates to the same parties as required for the initial Breach Reporting Form. The Business Associate is responsible for reporting all information needed by the DHA Privacy Office to enable timely and accurate determinations on reports to HHS as required by the HHS Breach Rule and reports to the Defense Privacy, Civil Liberties, and Transparency Division as required by DoD Privacy Program Issuances.

(b) Individual Notification Provisions

If the DHA Privacy Office determines that individual notification is required IAW 5 CFR §§ 164.400-414, the Business Associate shall provide written notification to individuals affected by the breach as soon as possible, but no later than ten working days after the breach is discovered and the identities of the individuals are ascertained. The ten-day period begins when the Business Associate determines the identities (including addresses) of the individuals whose records were affected.

The Business Associate's proposed notification to be issued to the affected individuals shall be submitted for approval to the DHA Privacy Office. Upon request, the Business Associate shall provide the DHA Privacy Office with the final text of the notification letter sent to the affected individuals. PII shall not be included with the text of the letter(s) provided... Copies of further correspondence with affected individuals need not be provided unless requested by the DHA Privacy Office. Pursuant to 45 CFR §§ 164.400-414 and section 13407 of the HITECH Act, the Business Associate's notification to the individuals, at a minimum, shall include the following:

—The individual(s) must be advised of what specific data was involved. It is insufficient to simply state that PII has been lost. Where names, Social Security Numbers (SSNs) or truncated SSNs, and Dates of Birth (DOBs) are involved, it is critical to advise the individual of the nature and extent of any potentially PHI data elements that have been breached. In all cases, individuals should be notified as to the nature and extent of any compromised PHI.

—The individual(s) must be informed of the facts and circumstances surrounding the breach. The description should be sufficiently detailed so that the individual clearly understands how the breach occurred.

—The individual(s) must be informed of any steps the individuals should take to protect themselves from potential harm resulting from the breach.

—The individual(s) must be informed of what protective actions the Business Associate is taking or the individual can take to mitigate against potential future harm. The notice must refer the individual to the current Federal Trade Commission

(FTC) web site pages on identity theft and the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); Teletype (TTY):): 1-866- 653-4261.

—The individual(s) must also be informed of any mitigation support services (e.g., one year of free credit monitoring, identification of fraud expense coverage for affected individuals, provision of credit freezes, etc.) that the Business Associate may offer affected individuals, the process to follow to obtain those services, and the period of time the services will be made available, and contact information (including a phone number, either direct or toll-free, e-mail address and postal address) for obtaining more information.

Business Associates shall ensure any envelope containing written notifications to affected individuals are clearly labeled to alert the recipient to the importance of its contents, e.g., "Data Breach Information Enclosed," and that the envelope is marked with the identity of the Business Associate and/or subcontractor organization that suffered the breach. The letter must also include contact information for a designated point of contact (POC),), phone number, email address, and postal address.

If the Business Associate determines that it cannot readily identify, or will be unable to reach, some affected individuals within the ten-day period after discovering the breach, the Business Associate shall so indicate in the initial or updated Breach Report Form. Within the 10-day period, the Business Associate shall provide the approved notification to those individuals who can be reached. Other individuals must be notified within ten days after their identities and addresses are ascertained. The Business Associate shall consult with the DHA Privacy Office, which will determine which media notice is most likely to reach the population not otherwise identified or reached. The Business Associate shall issue a generalized media notice(s) to that population in accordance with DHA Privacy Office approval.

The Business Associate shall, at no cost to the government, bear all costs associated with a breach of PII/PHI that the Business Associate has caused or is otherwise responsible for addressing.

VI. Termination

(a) Termination. Noncompliance by the Business Associate (or any of its staff, agents, or subcontractors) with any requirement addressed in this BAA may subject the Business Associate to termination under any applicable default or other termination provision of the Agreement.

(b) Effect of Termination.

(1) If the Agreement has records management requirements, the Business Associate shall handle such records in accordance with the records management requirements. If the Agreement does not have records management requirements, the records shall be handled in accordance with paragraphs (2) and (3) below, unless the Agreement has provisions for transfer of records and PII/PHI to a successor Business Associate, or if DHA gives directions for such transfer. In the case DHA or the Agreement provides for transfer of records, the Business Associate shall handle such records and information in accordance with such Agreement provisions or DHA direction.

(2) If the Agreement does not have records management requirements, except as provided in the following paragraph (3), upon termination of the Agreement, for any reason, the Business Associate shall return or destroy all PHI received from the Covered Entity or created or received by the Business Associate on behalf of the Covered Entity that the Business Associate still maintains in any form. This provision shall apply to PHI that is in the possession of subcontractors or agents of the Business Associate. The Business Associate shall retain no copies of the PHI or its derivatives.

(3) If the Agreement does not have records management provisions and the Business Associate determines that returning or destroying the PHI is infeasible, the Business Associate shall provide to the Covered

Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Covered Entity and the Business Associate that return, or destruction of PHI is infeasible, the Business Associate shall extend the protections of the Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as the Business Associate maintains such PHI.

VII. Execution

(a) Survival. The obligations of Business Associate under the "Effect of Termination" provision of this BAA shall survive the termination of the Agreement or any part thereof.

(b) Interpretation. Any ambiguity in the Agreement shall be resolved in favor of a meaning that permits the DoD Component and the Business Associate to comply with the HIPAA Rules and the DoD HIPAA Rules.