NOTICE TO CONTRACTOR

This is a combined synopsis/solicitation for commercial items prepared in accordance with the format in Revolutionary FAR Overhaul (RFO) Part 12.2, Solicitation, Evaluation, and Award. This announcement constitutes the only solicitation; quotes are being requested, and a separate written solicitation will not be issued. The solicitation number is **HT941026Q2045**. It is issued as a Request for Quote (RFQ). The solicitation document and incorporated provisions and clauses are those in effect through Federal Acquisition Circular (FAC) 2026-01 effective 03/13/2026 and Defense Federal Acquisition Regulation Supplement (DFARS) change 5/7/2026. The North American Industry Classification System (NAICS) Code for this acquisition is 513210. The size standard is $47.0 million dollars. The Product and Service Code (PSC) for this requirement is DA10. This solicitation is 100% set aside for small business. It is the responsibility of the contractor to be familiar with the applicable clauses and provisions.

This requirement is for non-personal services.

Defense Health Agency Contracting Activity (DHACA) Healthcare Contracting Division-West (HCD-W) requests responses from qualified sources capable of providing the following:

Laboratory document control software Subscription

Items required:

CLIN 0001:	Laboratory Document Control & Continuing Education – Base
Location:	60th MEDGRP DAVID GRANT (TRAVIS)
Period of Performance (POP):	1 Aug 2026 to 31 July 2027
Quantity:	1
Unit of Issue:	Job

CLIN 1001:	Laboratory Document Control & Continuing Education – Option 1
Location:	60th MEDGRP DAVID GRANT (TRAVIS)
Period of Performance (POP):	1 Aug 2027 to 31 July 2028
Quantity:	1
Unit of Issue:	Job

CLIN 2001:	Laboratory Document Control & Continuing Education – Option 2
Location:	60th MEDGRP DAVID GRANT (TRAVIS)
Period of Performance (POP):	1 Aug 2028 To: 31 July 2029
Quantity:	1
Unit of Issue:	Job

CLIN 3001:	Laboratory Document Control & Continuing Education – Option 3
Location:	60th MEDGRP DAVID GRANT (TRAVIS)
Period of Performance (POP):	1 Aug 2029 To: 31 July 2030
Quantity:	1
Unit of Issue:	Job

CLIN 4001:	Laboratory Document Control & Continuing Education – Option 4
Location:	60th MEDGRP DAVID GRANT (TRAVIS)

Period of Performance (POP): 1 Aug 2030 to 31 July 2031
Quantity: 1
Unit of Issue: Job

DEFENSE BIOMETRIC IDENTIFICATION SYSTEM (DBIDS)

(a) DBIDS is the current system for access control verification and management for the Department of Defense (DoD).

(b) DBIDS guidance for Vendors/Contractors to obtain a pass is accessible through the following website: https://www.cnic.navy.mil/Operations-and-Management/Base-Support/DBIDS/

(c) For more information or to enroll in the DBIDS Program, call: 1 (202) 433-4784. https://www.cnic.navy.mil/Operations-and-Management/Base-Support/DBIDS/

(d) Pre-enrolling will help expedite your processing time. To pre-enroll for a DBIDS card, visit the following website: https://dbids-global-enroll.dmdc.mil/preenrollui/

(e) Vendors, contractors, suppliers, and other service providers shall present their pass upon entry at the entry control point (ECP).

This acquisition incorporates by reference the following FAR provisions and clauses:

52.203-18	Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements-Representation (Jan 2017)
52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017)
52.204-7	System for Award Management (Oct 2018)
52.204-13	System for Award Management Maintenance (Oct 2018)
52.209-6	Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment
52.209-10	Prohibition on Contracting with Inverted Domestic Corporations
52.219-6	Notice of Total Small Business Set-Aside
52.222-3	Convict Labor
52.222-36	Equal Opportunity for Workers with Disabilities
52.222-42	Statement of Equivalent Rates for Federal Hires (MAY 2014)
52.222-43	Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (Multiple Year and Option Contracts) (AUG 2018)
52.222-50	Combating Trafficking in Persons (OCT 2025)
52.222-62	Paid Sick Leave Under Executive Order 13706 (JAN 2022)
52.222-90	Addressing DEI Discrimination by Federal Contractors (Deviation Date)
52.223-23	Sustainable Products and Services (DEVIATION) (MAR 2025)
52.225-25	Prohibition on Contracting with Entities Engaging in Certain Activities or Transactions Relating to Iran—Representation and Certifications (JUN 2020)
52.226-8	Encouraging Contractor Policies to Ban Text Messaging While Driving (MAY 2024)
52.232-33	Payment by Electronic Funds Transfer—System for Award Management (OCT 2018)

52.232-40 Providing Accelerated Payments to Small Business Subcontractors (NOV 2021)
52.233-3 Protest After Award (AUG 1996)
52.233-4 Applicable Law for Breach of Contract Claim (OCT 2004
52.232-18 Availability of Funds (Apr 1984)
52.240-90 Security Prohibitions and Exclusions Representations and Certifications
52.240-91 Security Prohibitions and Exclusions (DEC 2025)
52.240-93 Basic Safeguarding of Covered Contractor Information Systems (DEC 2025)

The following additional DFARS provisions and clauses applicable to this acquisition are incorporated by reference:

252.203-7000 Requirements Relating to Compensation of Former DoD Officials (Sep 2011)
252.203-7002 Requirement to Inform Employees of Whistleblower Rights (Dec 2022)
252.203-7005 Representation Relating to Compensation of Former DoD Officials (Sep 2022)
252.204-7019 Notice of NIST SP 800-171 DoD Assessment Requirements (Nov 2023)
252.204-7020 NIST SP 800-171 DoD Assessment Requirements (Nov 2023)
252.204-7022 Expediting Contract Closeout (May 2021)
252.204-7023 Reporting Requirements for Contracted Services (Jul 2021)
252.204-7024 Notice on the Use of the Supplier Performance Risk System (Mar 2023)
252.205-7000 Provision of Information to Cooperative Agreement Holders (OCT 2024)
252.225-7012 Preference for Certain Domestic Commodities (APR 2022)
252.225-7052 Restriction on the Acquisition of Certain Magnets, Tantalum, and Tungsten (MAY 2024)
252.225-7055 Representation Regarding Business Operations with the Maduro Regime (May 2022)
252.225-7056 Prohibition Regarding Business Operations with the Maduro Regime (Jan 2023)
252.225-7059 Prohibition on Certain Procurements from the Xinjiang Uyghur Autonomous Region–Representation (Jun 2023)
252.225-7060 Prohibition on Certain Procurements from the Xinjiang Uyghur Autonomous Region (Jun 2023)
252.226-7001 Utilization of Indian Organizations, Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns (JAN 2023)
252.232-7003 Electronic Submission of Payment Requests and Receiving Reports (Dec 2018)
252.232-7010 Levies on Contract Payments (Dec 2006)
252.237-7010 Prohibition on Interrogation of Detainees by Contractor Personnel (JAN 2023)
252.243-7002 Requests for Equitable Adjustment (DEC 2022)
252.244-7000 Subcontracts for Commercial Products or Commercial Services (Nov 2023)
252.247-7023 Transportation of Supplies by Sea—Basic (Oct 2024)

The following FAR provisions and clauses incorporated by full text apply to this acquisition:

52.212-1 INSTRUCTIONS TO OFFERORS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (SEP 2023)

(a) *North American Industry Classification System (NAICS) code and small business size standard*. The NAICS code(s) and small business size standard(s) for this acquisition appear elsewhere in the solicitation. However, the small business size standard for a concern that submits an offer, other than on a construction or service acquisition, but proposes to furnish an end item that it did not itself manufacture, process, or produce is 500 employees, or 150 employees for information technology value-added resellers under NAICS code 541519, if the acquisition—

(1) Is set aside for small business and has a value above the simplified acquisition threshold;

(2) Uses the HUBZone price evaluation preference regardless of dollar value, unless the offeror waives the price evaluation preference; or

(3) Is an 8(a), HUBZone, service-disabled veteran-owned, economically disadvantaged women-owned, or women-owned small business set-aside or sole-source award regardless of dollar value.

(b) *Submission of offers*. Submit signed and dated offers to the office specified in this solicitation at or before the exact time specified in this solicitation. Offers may be submitted on the SF 1449, letterhead stationery, or as otherwise specified in the solicitation. As a minimum, offers must show—

(1) The solicitation number;

(2) The time specified in the solicitation for receipt of offers;

(3) The name, address, and telephone number of the offeror;

(4) A technical description of the items being offered in sufficient detail to evaluate compliance with the requirements in the solicitation. This may include product literature, or other documents, if necessary;

(5) Terms of any express warranty;

(6) Price and any discount terms;

(7) "Remit to" address, if different than mailing address;

(8) A completed copy of the representations and certifications at Federal Acquisition Regulation (FAR) 52.212-3 (see FAR 52.212-3(b) for those representations and certifications that the offeror shall complete electronically);

(9) Acknowledgment of Solicitation Amendments;

(10) Past performance information, when included as an evaluation factor, to include recent and relevant contracts for the same or similar items and other references (including contract numbers, points of contact with telephone numbers and other relevant information); and

(11) If the offer is not submitted on the SF 1449, include a statement specifying the extent of agreement with all terms, conditions, and provisions included in the solicitation. Offers that fail to furnish required representations or information, or reject the terms and conditions of the solicitation may be excluded from consideration.

(c) *Period for acceptance of offers*. The offeror agrees to hold the prices in its offer firm for 30 calendar days from the date specified for receipt of offers, unless another time period is specified in an addendum to the solicitation.

(d) *Product samples*. When required by the solicitation, product samples shall be submitted at or prior to the time specified for receipt of offers. Unless otherwise specified in this solicitation, these samples

shall be submitted at no expense to the Government, and returned at the sender's request and expense, unless they are destroyed during preaward testing.

(e) *Multiple offers*. Offerors are encouraged to submit multiple offers presenting alternative terms and conditions, including alternative line items (provided that the alternative line items are consistent with FAR subpart 4.10), or alternative commercial products or commercial services for satisfying the requirements of this solicitation. Each offer submitted will be evaluated separately.

(f) *Late submissions, modifications, revisions, and withdrawals of offers*. (1) Offerors are responsible for submitting offers, and any modifications, revisions, or withdrawals, so as to reach the Government office designated in the solicitation by the time specified in the solicitation. If no time is specified in the solicitation, the time for receipt is 4:30 p.m., local time, for the designated Government office on the date that offers or revisions are due.

(2) (i) Any offer, modification, revision, or withdrawal of an offer received at the Government office designated in the solicitation after the exact time specified for receipt of offers is "late" and will not be considered unless it is received before award is made, the Contracting Officer determines that accepting the late offer would not unduly delay the acquisition; and-

(A) If it was transmitted through an electronic commerce method authorized by the solicitation, it was received at the initial point of entry to the Government infrastructure not later than 5:00 p.m. one working day prior to the date specified for receipt of offers; or

(B) There is acceptable evidence to establish that it was received at the Government installation designated for receipt of offers and was under the Government's control prior to the time set for receipt of offers; or

(C) If this solicitation is a request for proposals, it was the only proposal received.

(ii) However, a late modification of an otherwise successful offer, that makes its terms more favorable to the Government, will be considered at any time it is received and may be accepted.

(3) Acceptable evidence to establish the time of receipt at the Government installation includes the time/date stamp of that installation on the offer wrapper, other documentary evidence of receipt maintained by the installation, or oral testimony or statements of Government personnel.

(4) If an emergency or unanticipated event interrupts normal Government processes so that offers cannot be received at the Government office designated for receipt of offers by the exact time specified in the solicitation, and urgent Government requirements preclude amendment of the solicitation or other notice of an extension of the closing date, the time specified for receipt of offers will be deemed to be extended to the same time of day specified in the solicitation on the first work day on which normal Government processes resume.

(5) Offers may be withdrawn by written notice received at any time before the exact time set for receipt of offers. Oral offers in response to oral solicitations may be withdrawn orally. If the solicitation authorizes facsimile offers, offers may be withdrawn via facsimile received at any time before the exact time set for receipt of offers, subject to the conditions specified in the solicitation concerning facsimile offers. An offer may be withdrawn in person by an offeror or its authorized representative if, before the exact time set for receipt of offers, the identity of the person requesting withdrawal is established and the person signs a receipt for the offer.

(g) *Contract award (not applicable to Invitation for Bids)*. The Government intends to evaluate offers and award a contract without discussions with offerors. Therefore, the offeror's initial offer should contain the offeror's best terms from a price and technical standpoint. However, the Government reserves the right to conduct discussions if later determined by the Contracting Officer to be necessary. The Government may reject any or all offers if such action is in the public interest; accept other than the lowest offer; and waive informalities and minor irregularities in offers received.

(h) *Multiple awards*. The Government may accept any item or group of items of an offer, unless the offeror qualifies the offer by specific limitations. Unless otherwise provided in the Schedule, offers may not be submitted for quantities less than those specified. The Government reserves the right to make an award on any item for a quantity less than the quantity offered, at the unit prices offered, unless the offeror specifies otherwise in the offer.

(i) *Availability of requirements documents cited in the solicitation*.

(1) (i) The GSA Index of Federal Specifications, Standards and Commercial Item Descriptions, FPMR Part 101–29, and copies of Federal specifications, standards, and product descriptions can be downloaded from the ASSIST website at https://assist.dla.mil.

(ii) If the General Services Administration, Department of Agriculture, or Department of Veterans Affairs issued this solicitation, a copy of specifications, standards, and commercial item descriptions cited in this solicitation may be obtained from the address in paragraph (i)(1)(i) of this provision.

(2) Most unclassified Defense specifications and standards may be downloaded from the ASSIST website at https://assist.dla.mil.

(3) Defense documents not available from the ASSIST website may be requested from the Defense Standardization Program Office by—

(i) Using the ASSIST feedback module (https://assist.dla.mil/feedback); or

(ii) Contacting the Defense Standardization Program Office by telephone at 571–767–6688 or email at assisthelp@dla.mil.

(4) Nongovernment (voluntary) standards must be obtained from the organization responsible for their preparation, publication, or maintenance.

(j) *Unique entity identifier*. (Applies to all offers that exceed the micro-purchase threshold, and offers at or below the micro-purchase threshold if the solicitation requires the Contractor to be registered in the System for Award Management (SAM).) The Offeror shall enter, in the block with its name and address on the cover page of its offer, the annotation "Unique Entity Identifier" followed by the unique entity identifier that identifies the Offeror's name and address. The Offeror also shall enter its Electronic Funds Transfer (EFT) indicator, if applicable. The EFT indicator is a four-character suffix to the unique entity identifier. The suffix is assigned at the discretion of the Offeror to establish additional SAM records for identifying alternative EFT accounts (see FAR subpart 32.11) for the same entity. If the Offeror does not have a unique entity identifier, it should contact the entity designated at www.sam.gov for unique entity identifier establishment directly to obtain one. The Offeror should indicate that it is an offeror for a Government contract when contacting the entity designated at www.sam.gov for establishing the unique entity identifier.

(k) [Reserved]

(l) *Debriefing*. If a post-award debriefing is given to requesting offerors, the Government shall disclose the following information, if applicable:

(1) The agency's evaluation of the significant weak or deficient factors in the debriefed offeror's offer.

(2) The overall evaluated cost or price and technical rating of the successful and the debriefed offeror and past performance information on the debriefed offeror.

(3) The overall ranking of all offerors, when any ranking was developed by the agency during source selection.

(4) A summary of the rationale for award;

(5) For acquisitions of commercial products, the make and model of the product to be delivered by the successful offeror.

(6) Reasonable responses to relevant questions posed by the debriefed offeror as to whether source-selection procedures set forth in the solicitation, applicable regulations, and other applicable authorities were followed by the agency.

Addendum to FAR 52.212-1, Instructions to Offerors—Commercial Products and Commercial Services

The following is inserted as new paragraph (m) of the provision:

(m) QUOTER INSTRUCTIONS

The Government intends to award a firm-fixed-price (FFP) contract resulting from this RFQ to the responsible Quoter, whose quote conforms to the solicitation and is the most advantageous (best value) to the Government, price and other factors considered as defined in the EVALUATION FACTORS FOR AWARD section below. The Government will review the quotes received to determine if they are compliant with the RFQ requirements. A compliant quote is one that meets all of the terms, conditions, and specifications in the RFQ. The Quoter must provide all documents listed and comply with all RFQ instructions in order for their quote to be considered "compliant" with this RFQ. Only compliant quotes will be evaluated for award.

All questions regarding the RFQ, of a contractual or technical nature, must be submitted electronically by email to angelinemae.m.santiago.civ@health.mil no later than 1:00 pm Pacific on Friday, June 26th, 2026 . Questions submitted after the specified date and time may not receive a response. Questions, along with the Government's responses, will be posted as an attachment to the RFQ. Please be advised that the Government reserves the right to transmit those questions and answers of a common interest to all prospective Quoters.

Electronic Submission of Quotes:
Quotations shall be submitted electronically via email to angelinemae.m.santiago.civ@health.mil.

Quoters are instructed to electronically submit their complete quotation in one (1) single file, formatted in Portable Document Format (PDF) with a .pdf file extension as follows:

- FACTOR 1: Technical Capability:
Ability to meet the statement of work shall be demonstrated by the offeror's submission of a document that addresses how they will accomplish all applicable objectives, tasks and guidelines. The Quoter shall submit a capabilities statement, not to exceed two (2) pages, demonstrating the Quoter's technical capability to perform the required services in accordance with Attachment 1 (Performance Work Statement). The quoter shall specifically address each element identified under paragraph 1.4 and part 5 of the PWS.

Offerors are cautioned against restating PWS requirements in their proposal, particularly with regard to technical requirements; and must state how all requirements will be met. Statements such as "the offeror understands" and "the offeror shall/can comply", along with reference or industry references does not reflect that the offeror understands the requirements and will likely result in a diminished evaluation rating.

- FACTOR 2:
Past Performance:
The Quoter shall use Attachment 2 (Past Performance Questionnaire) to provide completed references for two (2) projects where you have provided RECENT and RELEVANT performance of the same or similar services required in this solicitation within the past three (3) years from the date of issuance of this RFQ. Past performance will be evaluated based on information from references provided and from authorized Government past performance systems and resources, including the Contractor Performance Assessment Rating System (CPARS).

RECENT is defined as services performed within the past three (3) years from the date of issuance of this RFQ. RELEVANT is defined as services the same as or similar to the services specified in the Performance Work Statement (PWS). Past performance information not meeting the above criteria will not be used for evaluation.

- FACTOR 3: Price:
The Quoter shall use Attachment 3 (Quote Sheet) to submit a firm-fixed-price for all contract line item numbers (CLINs) identified. Attachment 3 (Quote Sheet) and Pricing List shall be completed and signed, with acknowledgment of all amendments to the solicitation. No attempt to reformat or remove cells is authorized. Submission of pricing data shall be complete and accurate. Incomplete pricing may result in a Quoter's quotation being deemed ineligible for award.

- Completed Provisions:
Quoters shall be registered in the System for Award Management (SAM) with the appropriate NAICS code and completed representations and certifications and shall not have any active exclusions listed within SAM. Additionally, the Quoter shall include one (1) copy of the following FAR provision(s) located within this RFQ that shall be completed and included with the quote:

LATE SUBMISSIONS MAY NOT BE CONSIDERED.

It is a Quoter's responsibility, when transmitting its quote electronically, to ensure the quote's timely delivery by transmitting the quote sufficiently in advance of the time set for receipt of quotes to allow for timely receipt by the Government no later than the date and time stated in this RFQ. Quoters shall allow adequate time to upload files, which may be slower for non-DoD users, and to avoid other technical difficulties that may be encountered. A Quoter risks the late receipt and rejection of a quote where it

delays transmitting its quote until the last few minutes before the time set for receipt of quotes. Quotes that are received after the date and time stated in this RFQ will not be considered except at the discretion of the Contracting Officer; the Contracting Officer reserves full discretion to accept any late quotes at any time prior to award if it serves the best interest of the Government.

Quoters are responsible for submitting their quote in the format specified, consistent with requirements stated elsewhere in this RFQ. Quoters are asked to submit only the information required. Files that cannot be opened or are otherwise missing the required content are the responsibility of the Quoters. Submissions that do not adhere to format and content requirements may be considered non-compliant. The Government reserves the right to eliminate any such quotes from consideration for award.

Quotations must be received no later than 5:00 pm Pacific on Thursday, July 2, 2026.

(End of provision)

52.212-2 EVALUATION—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (NOV 2021)

(a) The Government will award a contract resulting from this solicitation to the responsible quoter whose quote conforming to the solicitation will be most advantageous to the Government, price and other factors considered. The following factors shall be used to evaluate quotes:

(1) Technical Capability
(2) Past Performance
(3) Price

Technical Capability will be rated on an Acceptable/Unacceptable basis, and Past Performance will be more important than price.

(b) Options. The Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. The Government may determine that an offer is unacceptable if the option prices are significantly unbalanced. Evaluation of options shall not obligate the Government to exercise the option(s).

(c) A written notice of award or acceptance of an offer, mailed or otherwise furnished to the successful offeror within the time for acceptance specified in the offer, shall result in a binding contract without further action by either party. Before the offer's specified expiration time, the Government may accept an offer (or part of an offer), whether or not there are negotiations after its receipt, unless a written notice of withdrawal is received before award.

Addendum to FAR 52.212-2, Evaluation—Commercial Products and Commercial Services

The following is inserted as new paragraph (d) of the provision:

(d) EVALUATION FACTORS FOR AWARD

Contract award shall be made on a "Past Performance Price Tradeoff" basis. This process allows for a tradeoff between past performance and price and allows the Government to accept other than the lowest priced quote or other than the highest rated quote to achieve a best-value contract award. This may result in an award to a higher-rated, higher-priced quote if the Government determines that the past performance

of the higher-priced quote outweighs the price difference. The selection process is subjective by nature and professional judgment is implicit throughout the tradeoff process.

The Quoter's technical capability will be evaluated to determine if it is acceptable or unacceptable in accordance with the evaluation criteria stated in this RFQ. If a Quoter's technical capability is determined to be unacceptable, the Quoter will no longer be considered for award. Award will be made to the Quoter providing a quote that is deemed most advantageous to the Government, whose technical capability has been determined to be "Acceptable" and trading off past performance against price. Past performance is more important than price.

The Government intends to award based on initial quotes. Notwithstanding this intent, the Contracting Officer reserves the right to conduct exchanges if it is within the best interest of the Government, a matter within their discretion.

Certified cost or pricing data is not required for commercial acquisitions or for acquisitions at or below the simplified acquisition threshold. However, if only one proposal is received, other than certified cost or pricing data may be required.

FACTOR 1: TECHNICAL CAPABILITY:

The Government will use the following ratings/descriptions in Table 1 when evaluating technical capability:

Table 1. Technical Capability Ratings

Rating	**Description**
Acceptable	Quote clearly demonstrates the Quoter's technical capability to perform the required services in accordance with the Performance Work Statement.
Unacceptable	Quote does not clearly demonstrate the Quoter's technical capability to perform the required services in accordance with the Performance Work Statement.

Offerors must receive an "Acceptable" rating on Factor 1, Technical Capability, in order to continue to Factor 2. Offerors that receive an "Unacceptable" rating on Factor 1 will not be evaluated any further and removed from further consideration for award.

FACTOR 2: PAST PERFORMANCE:

The Government will evaluate past performance by reviewing the Quoter's submitted past performance information and information from other sources that may include, but are not limited to, Government personnel and information retrieved through CPARS.

The past performance evaluation will result in an integrated assessment of the Quoter's probability of successfully performing the RFQ requirements. The past performance evaluation considers each Quoter's demonstrated recent and relevant record of performance in performing services the same as or similar to the services specified in the PWS. The Government will consider the recency and relevance of the information, the source of the information, context of the data, and general trends in the Quoter's

performance. The past performance confidence assessment rating is based on the Quoter's overall record of recency, relevancy, and quality of performance. These are combined to establish one performance confidence assessment rating for each Quoter.

The Government will use the following relevancy definitions in Table 2 when determining relevant past performance:

Table 2. Relevancy

Relevancy	**Definition**
Relevant	Past performance effort involved performance of services the same as or similar to the services specified in the PWS
Not Relevant	Past performance effort involved little or no performance of services the same as or similar to the services specified in the PWS.

The Government will use the following ratings/descriptions in Table 3 when evaluating past performance:

Table 3. Performance Confidence Assessment Ratings

Rating	**Description**
Substantial Confidence	Based on the Quoter's recent/relevant performance record, the Government has a high expectation that the Quoter will successfully perform the required effort.
Satisfactory Confidence	Based on the Quoter's recent/relevant performance record, the Government has a reasonable expectation that the Quoter will successfully perform the required effort.
Neutral Confidence	No recent/relevant performance record is available or the Quoter's performance record is so sparse that no meaningful confidence assessment rating can be reasonably assigned. The Quoter may not be evaluated favorably or unfavorably on the factor of past performance.
Limited Confidence	Based on the Quoter's recent/relevant performance record, the Government has a low expectation that the Quoter will successfully perform the required effort.
No Confidence	Based on the Quoter's recent/relevant performance record, the Government has no expectation that the Quoter will be able to successfully perform the required effort.

FACTOR 3: PRICE:

The Government will evaluate the quoted price for price reasonableness. The following price analysis techniques may be used to ensure a fair and reasonable price:

- Comparison of quoted prices received in response to the solicitation.
- Comparison of quoted prices with the independent Government estimate.
- Comparison of quoted prices with available historical information.
- Comparison of quoted prices with prices obtained through market research for the same or similar items.

The quoted price will be evaluated for the entire effort, inclusive of all options. Evaluation of options shall not obligate the Government to exercise the option(s).

Price must be determined fair and reasonable in order to be eligible for award. A price is reasonable if, in its nature and amount, it does not exceed that which would be incurred by a prudent person in the conduct of competitive business. A price that is found to be unreasonably high may be indicative of an inherent lack of understanding of the solicitation requirements and may result in the overall quote not being considered for award.

(End of provision)

52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within the period of performance of the contract.

(End of clause)

52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days prior to contract expiration; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 5 years.

(End of Clause)

52.232-34 PAYMENT BY ELECTRONIC FUNDS TRANSFER—OTHER THAN SYSTEM FOR AWARD MANAGEMENT (JUL 2013)

(a) Method of payment. (1) All payments by the Government under this contract shall be made by electronic funds transfer (EFT) except as provided in paragraph (a)(2) of this clause. As used in this clause, the term “EFT” refers to the funds transfer and may also include the payment information transfer.

(2) In the event the Government is unable to release one or more payments by EFT, the Contractor agrees to either--

(i) Accept payment by check or some other mutually agreeable method of payment; or

(ii) Request the Government to extend payment due dates until such time as the Government makes payment by EFT (but see paragraph (d) of this clause).

(b) Mandatory submission of Contractor's EFT information. (1) The Contractor is required to provide the Government with the information required to make payment by EFT (see paragraph (j) of this clause). The Contractor shall provide this information directly to the office designated in this contract to receive that information (hereafter: "designated office"') by the date when the contractor submitted first invoice, using EFT Form established by DFAS. If not otherwise specified in this contract, the payment office is the designated office for receipt of the Contractor's EFT information. If more than one designated office is named for the contract, the Contractor shall provide a separate notice to each office. In the event that the EFT information changes, the Contractor shall be responsible for providing the updated information to the designated office(s).

(2) If the Contractor provides EFT information applicable to multiple contracts, the Contractor shall specifically state the applicability of this EFT information in terms acceptable to the designated office. However, EFT information supplied to a designated office shall be applicable only to contracts that identify that designated office as the office to receive EFT information for that contract.

(c) Mechanisms for EFT payment. The Government may make payment by EFT through either the Automated Clearing House (ACH) network, subject to the rules of the National Automated Clearing House Association, or the Fedwire Transfer System. The rules governing Federal payments through the ACH are contained in 31 CFR part 210.

(d) Suspension of payment. (1) The Government is not required to make any payment under this contract until after receipt, by the designated office, of the correct EFT payment information from the Contractor. Until receipt of the correct EFT information, any invoice or contract financing request shall be deemed not to be a proper invoice for the purpose of prompt payment under this contract. The prompt payment terms of the contract regarding notice of an improper invoice and delays in accrual of interest penalties apply.

(2) If the EFT information changes after submission of correct EFT information, the Government shall begin using the changed EFT information no later than 30 days after its receipt by the designated office to the extent payment is made by EFT. However, the Contractor may request that no further payments be made until the updated EFT information is implemented by the payment office. If such suspension would result in a late payment under the prompt payment terms of this contract, the Contractor's request for suspension shall extend the due date for payment by the number of days of the suspension.

(e) Liability for uncompleted or erroneous transfers. (1) If an uncompleted or erroneous transfer occurs because the Government used the Contractor's EFT information incorrectly, the Government remains responsible for--

(i) Making a correct payment;

(ii) Paying any prompt payment penalty due; and

(iii) Recovering any erroneously directed funds.

(2) If an uncompleted or erroneous transfer occurs because the Contractor's EFT information was incorrect, or was revised within 30 days of Government release of the EFT payment transaction instruction to the Federal Reserve System, and--

(i) If the funds are no longer under the control of the payment office, the Government is deemed to have made payment and the Contractor is responsible for recovery of any erroneously directed funds; or

(ii) If the funds remain under the control of the payment office, the Government shall not make payment and the provisions of paragraph (d) shall apply.

(f) EFT and prompt payment. A payment shall be deemed to have been made in a timely manner in accordance with the prompt payment terms of this contract if, in the EFT payment transaction instruction released to the Federal Reserve System, the date specified for settlement of the payment is on or before the prompt payment due date, provided the specified payment date is a valid date under the rules of the Federal Reserve System.

(g) EFT and assignment of claims. If the Contractor assigns the proceeds of this contract as provided for in the assignment of claims terms of this contract, the Contractor shall require as a condition of any such assignment, that the assignee shall provide the EFT information required by paragraph (j) of this clause to the designated office, and shall be paid by EFT in accordance with the terms of this clause. In all respects, the requirements of this clause shall apply to the assignee as if it were the Contractor. EFT information that shows the ultimate recipient of the transfer to be other than the Contractor, in the absence of a proper assignment of claims acceptable to the Government, is incorrect EFT information within the meaning of paragraph (d) of this clause.

(h) Liability for change of EFT information by financial agent. The Government is not liable for errors resulting from changes to EFT information provided by the Contractor's financial agent.

(i) Payment information. The payment or disbursing office shall forward to the Contractor available payment information that is suitable for transmission as of the date of release of the EFT instruction to the Federal Reserve System. The Government may request the Contractor to designate a desired format and method(s) for delivery of payment information from a list of formats and methods the payment office is capable of executing. However, the Government does not guarantee that any particular format or method of delivery is available at any particular payment office and retains the latitude to use the format and delivery method most convenient to the Government. If the Government makes payment by check in accordance with paragraph (a) of this clause, the Government shall mail the payment information to the remittance address in the contract.

(j) EFT information. The Contractor shall provide the following information to the designated office. The Contractor may supply this data for this or multiple contracts (see paragraph (b) of this clause). The Contractor shall designate a single financial agent per contract capable of receiving and processing the EFT information using the EFT methods described in paragraph (c) of this clause.

(1) The contract number (or other procurement identification number).

(2) The Contractor's name and remittance address, as stated in the contract(s).

(3) The signature (manual or electronic, as appropriate), title, and telephone number of the Contractor official authorized to provide this information.

(4) The name, address, and 9-digit Routing Transit Number of the Contractor's financial agent.

(5) The Contractor's account number and the type of account (checking, saving, or lockbox).

(6) If applicable, the Fedwire Transfer System telegraphic abbreviation of the Contractor's financial agent.

(7) If applicable, the Contractor shall also provide the name, address, telegraphic abbreviation, and 9-digit Routing Transit Number of the correspondent financial institution receiving the wire transfer payment if the Contractor's financial agent is not directly on-line to the Fedwire Transfer System; and, therefore, not the receiver of the wire transfer payment.

(End of clause)

52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es):

https://www.acquisition.gov/browse/index/far
https://www.acquisition.gov/dfars

(End of provision)

52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

https://www.acquisition.gov/browse/index/far
https://www.acquisition.gov/dfars

(End of clause)

52.252-5 AUTHORIZED DEVIATIONS IN PROVISIONS (NOV 2020)

(a) The use in this solicitation of any Federal Acquisition Regulation (48 CFR Chapter 1) provision with an authorized deviation is indicated by the addition of “(DEVIATION)” after the date of the provision.

(b) The use in this solicitation of any Defense Federal Acquisition Regulation Supplement (48 CFR Chapter 2) provision with an authorized deviation is indicated by the addition of “(DEVIATION)” after the name of the regulation.

(End of provision)

52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (NOV 2020)

As prescribed in 52.107(f), insert the following clause in solicitations and contracts that include any FAR

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

(b) The use in this solicitation or contract of any Defense Federal Acquisition Regulation Supplement (48 CFR Chapter 2) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of clause)

252.232-7006 WIDE AREA WORKFLOW PAYMENT INSTRUCTIONS (JAN 2023)

(a) Definitions. As used in this clause—

"Department of Defense Activity Address Code (DoDAAC)" is a six position code that uniquely identifies a unit, activity, or organization.

"Document type" means the type of payment request or receiving report available for creation in Wide Area WorkFlow (WAWF).

"Local processing office (LPO)" is the office responsible for payment certification when payment certification is done external to the entitlement system.

"Payment request" and "receiving report" are defined in the clause at 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports.

(b) Electronic invoicing. The WAWF system provides the method to electronically process vendor payment requests and receiving reports, as authorized by Defense Federal Acquisition Regulation Supplement (DFARS) 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports.

(c) WAWF access. To access WAWF, the Contractor shall—

(1) Have a designated electronic business point of contact in the System for Award Management at https://www.sam.gov; and

(2) Be registered to use WAWF at https://wawf.eb.mil/ following the step-by-step procedures for self-registration available at this web site.

(d) WAWF training. The Contractor should follow the training instructions of the WAWF Web-Based Training Course and use the Practice Training Site before submitting payment requests through WAWF. Both can be accessed by selecting the "Web Based Training" link on the WAWF home page at https://wawf.eb.mil/.

(e) WAWF methods of document submission. Document submissions may be via web entry, Electronic Data Interchange, or File Transfer Protocol.

(f) WAWF payment instructions. The Contractor shall use the following information when submitting payment requests and receiving reports in WAWF for this contract or task or delivery order:

(1) Document type. The Contractor shall submit payment requests using the following document type(s):

(i) For cost-type line items, including labor-hour or time-and-materials, submit a cost voucher.

(ii) For fixed price line items—

(A) That require shipment of a deliverable, submit the invoice and receiving report specified by the Contracting Officer.

(B) For services that do not require shipment of a deliverable, submit either the Invoice 2in1, which meets the requirements for the invoice and receiving report, or the applicable invoice and receiving report, as specified by the Contracting Officer.

2 IN 1 SERVICES ONLY

(iii) For customary progress payments based on costs incurred, submit a progress payment request.

(iv) For performance based payments, submit a performance based payment request.

(v) For commercial financing, submit a commercial financing request.

(2) Fast Pay requests are only permitted when Federal Acquisition Regulation (FAR) 52.213-1 is included in the contract.

[Note: The Contractor may use a WAWF "combo" document type to create some combinations of invoice and receiving report in one step.]

(3) Document routing. The Contractor shall use the information in the Routing Data Table below only to fill in applicable fields in WAWF when creating payment requests and receiving reports in the system.

Routing Data Table

Field Name in WAWF	***Data to be entered in WAWF***
Pay Official DoDAAC	HQ0490
Issue By DoDAAC	**HT9410**
Admin DoDAAC	**HT9410**
Inspect By DoDAAC	N/A
Ship To Code	HT1102
Ship From Code	**N/A**
Mark For Code	**N/A**
Service Approver (DoDAAC)	HT1102
Service Acceptor (DoDAAC)	HT1102
Accept at Other DoDAAC	**N/A**

LPO DoDAAC	**N/A**
DCAA Auditor DoDAAC	**N/A**
Other DoDAAC(s)	**N/A**

(4) Payment request. The Contractor shall ensure a payment request includes documentation appropriate to the type of payment request in accordance with the payment clause, contract financing clause, or Federal Acquisition Regulation 52.216-7, Allowable Cost and Payment, as applicable.

(5) Receiving report. The Contractor shall ensure a receiving report meets the requirements of DFARS Appendix F.

(g) WAWF point of contact.

(1) The Contractor may obtain clarification regarding invoicing in WAWF from the following contracting activity's WAWF point of contact.

WAWF Acceptor Name: SrA Wayne Johnson
WAWF Acceptor Email: wayne.v.johnson6.mil@health.mil

(2) Contact the WAWF helpdesk at 866-618-5988, if assistance is needed.

(End of clause)

The following Defense Health Agency (DHA) Procedures, Guidance, and Information (PGI) apply to this acquisition:

DHA PGI 203.104-7 VIOLATIONS OR POSSIBLE VIOLATIONS (January 23, 2020)

IMPROPER BUSINESS PRACTICES AND PERSONAL CONFLICTS OF INTEREST

INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS

1. The Offeror's attention is directed to FAR, Part 3 and DFARS, Part 203, "Improper Business Practices and Personal Consultant Conflicts of Interest."

2. DFARS 252.203-7005 Representation Relating to Compensation of Former DoD Officials (Nov 2011)

(a) Definition. "Covered DoD official" is defined in the clause at 252.203-7000, Requirements Relating to Compensation of Former DoD Officials.

(b) By submission of this offer, the offeror represents, to the best of its knowledge and belief, that all covered DoD officials employed by or otherwise receiving compensation from the offeror, and who are expected to undertake activities on behalf of the offeror for any resulting contract, are presently in compliance with all post-employment restrictions covered by 18 U.S.C. 207, 41 U.S.C. 2101-2107, and 5 CFR parts 2637 and 2641, including Federal Acquisition Regulation 3.104-2.

(End of provision)

DHA PGI 211.106 PURCHASE DESCRIPTIONS FOR SERVICE CONTRACTS (April 4, 2014)

PROPER IDENTIFICATION OF CONTRACTOR PERSONNEL

1. Contractors, including subcontractors at all tiers, shall provide for a clear distinction from Government personnel. Contractor employees shall not act, advertise, or presume to be Government employees, agents, or representatives. Contractor employees are required to appropriately identify themselves as contractor employees at all times, including in telephone conversations, formal and informal written correspondence, paper and electronic, and in any other situation where their actions could be construed as acts of Government officials, unless, in the judgment of the Government, no harm can come from failing to identify themselves. Contractor employees shall be introduced as contractor personnel and display distinguishing visible identification at all times whether in conversations, meetings, or other forms of communication with Government personnel.

2. Contractor personnel, while performing in a contractor capacity, shall refrain from using their retired or reserve component military rank or title (if applicable) in written or verbal communications associated with the contracts for which they provide services.

3. The Contractor shall incorporate the substance of this requirement in all subcontracts awarded under this contract.

(End of requirements language)

DHA PGI 233.103-90 AGENCY LEVEL PROTESTS (March 22, 2020)

An interested party filing a protest with Defense Health Agency (DHA) has the option of requesting review by either the Contracting Officer (CO) or an independent review Official (IRO), who is a DHA official at a level above the CO. Alternately, an interested party may request IRO review as an appeal of the CO's protest decision.

Where applicable, an interested party must clearly state in the protest that IRO review is requested, and must specify the nature of the independent review sought – whether as an alternative to CO review or as an appeal of the CO's decision.

Regardless of which review is requested, all protests must be complete and submitted to the CO within the timeframes specified in FAR Subpart 33.1.

(End of DHA language)

<u>The following DHA Standard Language applies to this acquisition</u>:

Personally Identifiable Information, Protected Health Information, and Federal Information Requirements
(Revised 10/27/2020)

1. General Requirements Overview - Personally Identifiable Information (PII), Protected Health Information (PHI) and Federal Information Laws

This Section addresses the Contractor's requirements under The Privacy Act of 1974 (Privacy Act), The Freedom of Information Act (FOIA), and The Health Insurance Portability and Accountability Act (HIPAA) as set forth in applicable statutes, implementing regulations and Department of Defense (DoD) issuances. In general, the Contractor shall comply with the specific requirements set forth in this Section and elsewhere in this Contract. The Contractor shall also comply with requirements relating to records management as described herein.

This Contract incorporates by reference the federal regulations and DoD issuances referred to in this Section. If any authority is amended or replaced, the changed requirement is effective when it is incorporated under contract change procedures. Where a federal regulation and any DoD issuance govern the same subject matter, the Contractor shall first follow the more specific DoD implementation unless the DoD issuance does not address or is unclear on that matter. DoD issuances are available at http://www.dtic.mil/whs/directives.

For purposes of this Section, the following definitions apply.

DoD Privacy Act Issuances means the DoD issuances implementing the Privacy Act, which are DoDI 5400.11, DoD Privacy and Civil Liberties Programs, January 29, 2019, and DoDI 5400.11- R, Department of Defense Privacy Program, May 14, 2007.

HIPAA Rules means, collectively, the HIPAA Privacy, Security, Breach, and Enforcement Rules, issued by the U.S. Department of Health and Human Services (HHS) and codified at 45 Code of Federal Regulations (CFR) Part 160 and Part 164, Subpart E (Privacy), Subpart C (Security), Subpart D (Breach) and Part 160, Subparts C-E (Enforcement), as amended.
Additional HIPAA rules regarding electronic transactions and code sets (45 CFR Part 162) are not addressed in this Section and are not included in the term HIPAA Rules.

DoD HIPAA Issuances means the DoD issuances implementing the HIPAA Rules in the DoD Military Health System (MHS). These issuances are DoDM 6025.18, "Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs," March 13, 2019, 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.

Defense Health Agency (DHA) Privacy Office is the DHA Privacy and Civil Liberties Office. The DHA Privacy Office Chief is the HIPAA Privacy and Security Officer for DHA.

2. Records Management

When creating and maintaining official government records, the Contractor shall comply with all federal requirements established by 44 United States Code (U.S.C.) Chapters 21, 29, 31, 33 and 35, and by 36 CFR, Chapter XII, Subchapter B – Records Management. The Contractor shall also comply with DoD Administrative Instruction No. 15 (DoD AI-15), "OSD Records and Information Management Program" (May 3, 2013) and Records Management requirements outlined in the current TRICARE Operations Manual (TOM).

3. Freedom of Information Act (FOIA)

The Contractor shall comply with the following procedures if it receives a FOIA request and immediately contact the DHA FOIA Officer for evaluation/action:

The Contractor shall inform beneficiaries that DHA FOIA procedures require a written request preferably sent via the National FOIA Portal at: www.FOIA.gov. However, requesters may also submit requests via email at DHA.FOIA@mail.mil; or via postal delivery addressed to the DHA Freedom of Information Service Center, 7700 Arlington Boulevard, Suite 5101, Falls Church, Virginia 22042-5101. All FOIA requests shall describe the desired record as completely as possible to facilitate its retrieval from files and to reduce search fees which may be borne by the requestor. Contract and/or Modification numbers must be included in all FOIA requests seeking DHA procurement records. Although the administrative time limit to grant or deny a request (ten working days after receipt) does not begin until the request is received by DHA, the Contractor shall act as quickly as possible and respond to DHA within ten working days.

In response to requests received by the Contractor for the release of information, unclassified information, documents, and forms which were previously provided to the public as part of routine services shall continue to be made available in accordance with previously established criteria. All other requests from the public for release of DHA records and, specifically, all requests that reference FOIA shall be immediately forwarded to DHA, ATTENTION: Freedom of Information Officer, for appropriate action. Direct contact, including interim replies, between TRICARE contractors and such requestors is not authorized. The Contractor shall process requests by individuals for access to records about themselves in accordance with directions from the DHA Freedom of Information Service Center. If such a requestor specifically makes the request under the Privacy Act or does not make clear whether the request is made under FOIA or the Privacy Act, the Contractor shall process the request in accordance with directions from the DHA Privacy Office. If requestor specifically seeks PHI under HIPAA, the Contractor shall follow paragraph 8.1.6, relating to individual rights of access to PHI.

4. Systems of Records

In order to meet the requirements of the Privacy Act and the DoD Privacy Act Issuances, the Contractor shall identify to the DHA Contracting Officer (CO) systems of records that are or will be maintained or operated for DHA where records of PII collected from individuals are maintained and specifically retrieved using a personal identifier. Upon identification of such systems to the CO, and prior to the lawful operation of such systems, the Contractor shall coordinate with the DHA Privacy Office to complete systems of records notices (SORNs) for submission and publication in the *Federal Register* as coordinated by the Defense Privacy, Civil Liberties, and Transparency Division, and as required by the DoD Privacy Act Issuances.

Following proper SORN publication and Government confirmation of Contractor authority to operate the applicable system(s), the Contractor shall also comply with the additional systems of records and SORN guidance, in coordination with the DHA Privacy Office, regarding periodic system review, amendments, alterations, or deletions set forth by the DoD Privacy Act Issuances, Office of Management and Budget (OMB) Memorandum 99-05, Attachment B, OMB Circular A-130, and Privacy Act of 1974 requirements applicable to contractors operating systems of records on behalf of federal agencies. The Contractor shall promptly advise the DHA Privacy Office of changes in systems of records or their use that may require a change in the SORN.

5. Privacy Impact Assessment (PIA)

If DHA data is stored on a Contractor owned system, a PIA is required from the Contractor.

6. Data Sharing Agreement (DSA)

6.1 (Applies if contract requirements involve the use of DHA data (including PII/PHI, a limited data set, or de-identified data)

The Contractor shall consult with the DHA Privacy Office to determine if the Contractor must obtain a DSA or Data Use Agreement (DUA), when DHA data will be accessed, used, disclosed, or stored, to perform the requirements of this Contract.

The Contractor shall comply with the permitted uses established in a DSA/DUA to prevent the unauthorized use and/or disclosure of any PII/PHI, in accordance with the HIPAA Rules and DoD HIPAA Issuances. Likewise, the Contractor shall comply with the DoD Privacy Act Issuances.

Prior to using any data involving PHI for research purposes, as defined by HIPAA, the Contractor must gain approval from the DHA Privacy Board. Thus, the Contractor shall comply with DHA Privacy Board requests for additional documentation.

To begin the DSA request process, the Contractor shall submit a DSA Application (DSAA) to the DHA Privacy Office. Upon approval, the requestor shall enter into one of the following agreements, depending on the data involved:

- DSA for De-Identified Data
- DSA for PHI
- DSA for PII Without PHI
- DUA for Limited Data Set

DSAs executed for contract support will expire after 1 year or at the end of the contract option year, whichever comes first. If the contractual use of DHA data will continue after the DSA expiration date, the Contractor shall submit a DSA Renewal Request template to the Privacy Office; however, if the DSA will not be renewed, the Contractor shall close the DSA by providing a Certificate of Data Disposition (CDD) to the DHA Privacy Office.

6.2 (Applies if contract requirements may include human subject research)

This Contract incorporates by reference the Protection of Human Subject Research clause in the Defense Federal Acquisition Regulation Supplement (DFARS) at 48 CFR 252.235-7004. A separate DFARS provision, 48 CFR 235.072(e), requires that the clause be incorporated in contracts that include or may include research involving human subjects in accordance with 32 CFR 219, DoDI 3216.02, and 10 U.S.C. 980, including research that meets exemption criteria under 32 CFR 219.101(b), the clause applies to solicitations and contracts awarded by any DoD component, regardless of mission or funding Program Element Code. Thus, in the event a contractor participates in a study or demonstration project or other activity that involves human subject research, then the contractor shall comply with Protection of Human Subject Research clause. COs may not determine whether an activity is exempt from human subject research requirements. If contractor activity appears to involve human subject research, then the contractor shall consult the DHA Privacy Office, which may contact the Research Regulatory Oversight Office in the Office of the Under Secretary of Defense for Personnel and Readiness (OUSD(P&R)).

7. Privacy Act and HIPAA Training

The Contractor shall ensure that its entire staff, including subcontractors and consultants that perform

work on this Contract receive training on the Privacy Act, HIPAA, and the federal regulations on confidentiality of substance use disorder patient records, 42 CFR Part 2. Refer to FAR 52.224-3 regarding specific requirements for Privacy Training appropriate to the
Contractor's scope of involvement with DHA's PHI and its regulatory responsibilities as either a Covered Entity, or Business Associate.

The Contractor shall ensure all employees and subcontractors supply a certificate of all training completion to the Contracting Officer's Representative (COR) within 30 days of being assigned and on an annual basis based on the trainee's birth month thereafter.

8. HIPAA Business Associate Provisions

8.1 Business Associate – General Provisions

The Contractor meets the definition of Business Associate, and DHA meets the definition of a covered entity under the HIPAA Rules and the DoD HIPAA Issuances. Therefore, a Business Associate Agreement (BAA) between the Contractor and DHA is required to comply with the HIPAA Rules and the DoD HIPAA Issuances. The contractor shall use the DoD BAA, which shall be used by all organizational entities within the DoD, referred to collectively as the "DoD Components", located at https://www.health.mil/Military-Health-Topics/Privacy-and-Civil- Liberties/Privacy-Contract-Language/HIPAA-Compliant-Business-Associate-Agreement-for-the-MHS.

9. Breach Response

[This paragraph 9 is inoperative, and all references herein to "paragraph 9" shall be deemed to refer to the TOM breach responses provisions, if the contract incorporates the TOM by reference.]

9.1 Definitions Related to Breach response

9.1.2 **Breach** means a 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 PII; or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose. The foregoing definition is based on the definition of breach in DoDM 6025.18. Breaches are classified as either possible or confirmed (see the following two definitions) and as either cyber or non-cyber (i.e., involving either electronic PII/PHI or paper/oral PII/PHI).

9.1.3 A **possible breach** is an incident where the possibility of unauthorized access is suspected (or should be suspected) and has not been ruled out. For example, if a laptop containing PII/PHI is lost, and the contractor does not initially know whether or not the PII/PHI was encrypted, then the incident must initially be classified as a possible breach, because it is impossible to rule out the possibility of unauthorized access to the PII/PHI. In contrast, that possibility can be ruled out immediately, and a possible breach has not occurred, when misdirected postal mail is returned unopened in its original packaging. However, if the intended recipient informs the contractor that an expected package has not been received, then a possible breach exists until and unless the unopened package is returned to the contractor. In determining whether unauthorized access should be suspected, the contractor shall consider at least the following factors:

- How the event was discovered;
- Did the information stay within the covered entity's control;
- Was the information actually accessed/viewed; and

- Ability to ensure containment (e.g., recovered, destroyed, or deleted).

9.1.4 A **confirmed breach** is an incident in which it is known that unauthorized access could occur. For example, if a laptop containing PII/PHI is lost and the contractor knows that the PII/PHI is unencrypted, then the contractor should classify and report the incident as a confirmed breach, because unauthorized access could occur due to the lack of encryption (the contractor knows this even without knowing whether or not unauthorized access to the PII/PHI has actually occurred). If the laptop is subsequently recovered and forensic investigation reveals that files containing PII/PHI were never accessed, then the possibility of unauthorized access can be ruled out, and the contractor should re-classify the incident as a non-breach incident.

9.1.5 A **HHS breach** is an incident that satisfies the definition of breach in Section 164.402 of the HIPAA Breach Rule. The text of the HHS definition states:

Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of this part [i.e., the HIPAA Privacy Rule] which compromises the security or privacy of the PHI.

HHS breach excludes:

> Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a DoD covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule.
>
> Any inadvertent disclosure by a person who is authorized to access PHI at a DoD covered entity or business associate to another person authorized to access PHI at the same DoD covered entity or business associate, or organized health care arrangement in which the DoD covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by the HIPAA Privacy Rule.
>
> A disclosure of PHI where a DoD covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Except as provided in this definition, an acquisition, access, use, or disclosure of PHI in a manner not permitted under this issuance is presumed to be a breach unless the DoD covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

> The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
>
> The unauthorized person who used the PHI or to whom the disclosure was made; Whether the PHI was actually acquired or viewed; and
> The extent to which the risk to the PHI has been mitigated.

9.1.6 A **cybersecurity incident** is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices, with respect to electronic PII/PHI. A cybersecurity incident may or may not involve a breach of PII/PHI. For example, a malware infection would be a possible breach if it could cause unauthorized access to PII/PHI. However, if the malware only

affects data integrity or availability (not confidentiality), then a non-breach cybersecurity incident has occurred.

9.2 General

9.2.1 The breach response requirements shall be followed for all unauthorized use or disclosure of information regardless of whether the information is PHI or solely PII.

9.2.2 Because DoD defines "breach" to include possible (suspected), as well as actual (confirmed) breaches, the Contractor shall implement these breach response requirements immediately upon the Contractor's discovery of a possible breach. These procedures focus on the first two steps (breach identification and reporting) of a comprehensive breach response program, but also require addressing the remaining steps: containment, mitigation (which includes individual notification), eradication, recovery, and follow-up.

9.2.3 The contractor shall establish internal processes for carrying out the procedures set forth below. These processes shall assign responsibility for investigating, classifying, reporting, and otherwise responding to breaches and cybersecurity incidents. The contractor should consult with the DHA Privacy Office where guidance is needed, such as when the contractor is uncertain whether a discovered breach is the contractor's responsibility (e.g., if the contractor discovers a breach not caused by the contractor), or how the contractor is to classify an incident (breach vs. non-breach, confirmed vs. possible, cyber vs. non-cyber). Under no circumstances will a contractor delay reporting a confirmed or possible breach to the DHA Privacy Office beyond the 24-hour deadline. In conjunction with its initial investigation, the contractor shall immediately take steps to minimize any impact from the occurrence, proceed with further investigation of any relevant details (such as root causes, vulnerabilities exploited), and initiate further breach response steps.

9.2.4 In the event of a cybersecurity incident not involving a PII/PHI breach, the contractor shall follow applicable DoD cybersecurity and NIST requirements, which include United States- Computer Emergency Readiness Team (US-CERT) reporting (see paragraph 9.3). If at any point a contractor finds that a cybersecurity incident involves a PII/PHI breach (possible or confirmed), the contractor shall immediately initiate the reporting procedures set forth below. The contractor shall also continue to follow any required cybersecurity incident response procedures and other applicable DoD cybersecurity requirements.

9.2.5 Contractors shall require subcontractors who discover a possible breach or cybersecurity incident to initiate the incident response requirements herein by reporting the incident to the contractor immediately after discovery. The time of that report to the contractor shall trigger the contractor's DHA Privacy Office reporting deadline (24 hours) under paragraph 9.3.2. If a cybersecurity incident is involved, the contractor's deadline for US-CERT reporting (1 hour) runs from the time the incident is confirmed. The contractor shall require the subcontractor to cooperate as necessary to meet these deadlines, maintain records, and otherwise enable the contractor to complete the breach response requirements herein. Alternatively, the contractor and subcontractor may agree that the subcontractor shall report directly to US-CERT and the DHA Privacy Office, and that the subcontractor shall be responsible for completing the response process, provided that such agreement requires the subcontractor to inform the contractor of the incident and the subsequent response actions.

9.2.6 Contractors shall maintain records of all breach and cybersecurity incident investigations, regardless of the outcome. Investigations identifying unauthorized disclosures must be logged for HIPAA and Privacy Act disclosure accounting purposes, whether or not individual notification is required under

the HIPAA Breach Rule.

9.2.7 Contractors, when acting as HIPAA-covered entities, and not as business associates, are not subject to the breach response requirements herein. However, such contractors are subject to both the HIPAA Breach Rule (applicable to them in their capacity as covered entities) and DoD cybersecurity requirements (applicable to them in their capacity as DoD contractors).

9.3 Reporting Provisions

9.3.1 Immediately upon discovery of a possible or confirmed breach or cybersecurity incident, the contractor shall initiate an investigation. If the incident involves electronic PII/PHI, and if the investigation finds a confirmed breach or cybersecurity incident, the contractor shall report it, within 1 hour of confirmation, to the US-CERT Incident Reporting System at https://forms.us-cert.gov/report/, as required by the Department of Homeland Security (DHS).

Note: DHS no longer requires US-CERT reporting of non-cyber breaches or unconfirmed electronic breaches. However, DHS permits US-CERT reporting of unconfirmed cyber-related incidents on a voluntary basis. Thus, if a contractor is uncertain whether a possible cyber-related incident should be treated as confirmed and thus reportable, the contractor may voluntarily report the incident.

Before submission to US-CERT, the contractor shall save a copy of the on-line report. After submitting the report, the contractor shall record the US-CERT incident reporting number, which shall be included in the initial report to the DHA Privacy Office as described in paragraph 9.3.2.

Note: Regardless of whether or not an incident is confirmed as a breach, the contractor must also investigate whether or not the incident impacts data integrity or availability of PII/PHI. If such impact is confirmed, then the incident is reportable to US-CERT as a cybersecurity incident. For guidance on investigating the impact on data integrity and availability, refer to DoD cybersecurity and NIST guidance.

The contractor shall provide any updates to the initial US-CERT report by email to soc@us-cert.gov, with the Reporting Number in the subject line. The contractor shall provide a copy of the initial or updated US-CERT report to the DHA Privacy Office if requested. Contractor questions about US-CERT reporting shall be directed to the DHA Privacy Office, not the US-CERT office.

9.3.2 In addition to US-CERT reporting, the contractor shall report to the DHA Privacy Office by submitting the form specified below within 24 hours of discovery of a breach (possible or confirmed), unless the breach falls within a category that the Privacy Office has determined to be not reportable. This 24-hour period runs from the time of discovery, unlike the 1-hour US-CERT reporting period, which runs from the time a cybersecurity incident is confirmed. Thus, depending on the time period needed to confirm, the report to the DHA Privacy Office may be due either before or after the US-CERT report.

The breach report form required within the 24-hour deadline shall be sent by e-mail to: DHA.PrivacyOfficer@mail.mil. The contractor shall also e-mail the report to the CO, the COR, and its usual point of contact at the applicable Program Office. Encryption is not required, because reports and notices shall not contain PII/PHI. If electronic mail is not available, telephone notification is also acceptable (at 703-275-6363), but all notifications and reports delivered telephonically must be confirmed in writing as soon as technically feasible.

Contractors shall prepare the breach reports required within the 24-hour deadline by completing the Breach Reporting Department of Defense Form DD 2959 (Breach of PII Report), available at

https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd2959.pdf. For non-cyber incidents without a US-CERT number, the contractor shall assign an internal tracking number and include that number in Box 1.e of the DD Form 2959. The contractor shall coordinate with the DHA Privacy Office for subsequent action, such as beneficiary notification, and mitigation. The contractor must promptly update the DD Form 2959 as new information becomes available.

When a Breach Report Form initially submitted is incomplete or incorrect due to unavailable information, or when significant developments require an update, the Contractor shall submit a revised form or forms promptly after the new information becomes available, stating the updated status and previous report date(s) and showing any revisions or additions in red text. The Contractor shall provide updates to the same parties as required for the initial Breach Report Form.

9.4 Individual Notification Provisions

9.4.1 If the DHA Privacy Office determines that individual notification is required, the Contractor shall provide written notification to beneficiaries affected by the breach as soon as possible, but no later than 10 working days after the breach is discovered and the identities and addresses of the beneficiaries are ascertained. The 10-day period begins when the Contractor is able to determine the identities (including addresses) of the beneficiaries whose records were impacted. If notification cannot be accomplished within 10 working days, the contractor shall notify the DHA Privacy Office.

9.4.2 The Contractor's proposed notification to be issued to the affected beneficiaries shall be submitted to the DHA Privacy Office for approval. The notification to beneficiaries shall include, at a minimum, the following:

- Specific data elements,
- Basic facts and circumstances,
- Recommended precautions the beneficiary can take,
- Federal Trade Commission (FTC) identity theft hotline information, and
- Any mitigation support services offered, such as credit monitoring.

Contractors 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 Contractor and/or subcontractor organization that suffered the breach.

If media notice is required, the contractor will submit a proposed notice and suggested media outlets for the DHA Privacy Office review and approval (which will include coordination with the DHA Communications Division).

9.5 In the event the Contractor is uncertain on how to apply the above requirements, the Contractor shall consult with the CO, who will consult with the Privacy Office as appropriate when determinations on applying the above requirements are needed.

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

(End of PII, PHI, and Federal Information Requirements)

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; 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 that 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 Associate's 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 (PII); or (2) an authorized user accesses or potentially accesses PII for an other 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 Part V 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.

(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

(a) 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 at

https://www.cnss.gov/CNSS/issuances/Instructions.cfm, the discovering party shall report the breach to the DHA NIWC CSSP Watchdesk 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 Watchdesk 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 at 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/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.

_____	_____
[Business Associate]	[DoD Covered Entity]
_____	_____
Date	Date

(End of BAA)

******* End of Combined Synopsis/Solicitation ********