SUBJECT: Enterprise Mammography Tracking and Reporting System

GENERAL INFORMATION

CONTRACTING OFFICE'S ZIP CODE:	07724
SOLICITATION NUMBER:	36C10B26R0035
RESPONSE DATE/TIME/ZONE:	08-20-2026 9:00:00 AM Eastern Time, New York, USA
ARCHIVE:	60 days after the response date
RECOVERY ACT FUNDS:	N
SET-ASIDE:	
PRODUCT SERVICE CODE:	6525
NAICS CODE:	513210
CONTRACTING OFFICE ADDRESS:	Department of Veterans Affairs Technology Acquisition Center 23 Christopher Way Eatontown NJ 07724
POINT OF CONTACTS:	Contract Specialist: Terricia Lloyd; Terricia.Lloyd@va.gov Contracting Officer: Brett Schwerin, Brett.Schwerin@va.gov

PLACE OF PERFORMANCE

ADDRESS	
POSTAL CODE	
COUNTRY	USA

ADDITIONAL INFORMATION

AGENCY'S URL	
URL DESCRIPTION	
AGENCY CONTACT'S EMAIL ADDRESS	
EMAIL DESCRIPTION	

DESCRIPTION

This is a combined synopsis/solicitation for commercial products or commercial services prepared in accordance with the Revolutionary Federal Acquisition Overhaul (RFO) Class Deviation Part 12, as supplemented with additional information included in this notice. This announcement constitutes the only solicitation; proposals are being requested and an additional solicitation will not be issued.

The Request for Proposal (RFP) contains all applicable solicitation information pertinent to this acquisition; offerors must review the RFP in its entirety

1. Title: Enterprise Mammography Tracking and Reporting System

2. RFP: 36C10B26R0035

3. Solicitation Issue Date: August 10, 2026.

4. The solicitation document and incorporated provisions and clauses are those in effect through Federal Acquisition Circular 2026-01, effective March 13, 2026. The full text of provisions and clauses may be accessed electronically at https://www.acquisition.gov/far-overhaul/far-part-deviation-guide.

5. Solicitation is unrestricted under the North American Industry Classification System Code, 513210, Software Publishers, with associated business size standard of $47M.

6. The following are the Terms and Conditions for RFP 36C10B26R0035. Any resultant award will be issued on a Standard Form 1449 and will include Sections B, C, and D; Section E will be removed at time of award.

7. See the RFP for the following information:

    a. Price Schedule for line items numbers, description, quantities, and units of measure (including options and optional tasks).
    b. Dates, places of delivery and acceptance
    c. Performance Work Statement for requirements description
    d. Performance Periods
    e. Solicitation Section B.3 below regarding requirements for Software License, Maintenance, and Technical Support.
    f. Clause RFO 52.212-4, Terms and Conditions - Commercial Products and Commercial Services.
    g. Provision RFO 52.212-1, Instructions to Offerors - Commercial Products and Commercial Services.
    h. Provision 52.212-2, Evaluation - Commercial Products and Commercial Services
    i. Solicitation Provision E.12, “Basis for Award” which includes the specific evaluation criteria to be used for this acquisition.
    j. Other terms and conditions.

8. Questions Due Date:

   Questions are due no later than **12:00:00 pm on August 14, 2026**. Questions must be submitted to Contract Specialist Terricia Lloyd, Terricia.Lloyd@va.gov, and Contracting Officer, Brett Schwerin, Brett.Schwerin@va.gov.

9. Proposal Due Date:

   Submissions are due no later than **09:00:00 am on August 20, 2026.** To avoid submission of late proposals, we recommend proposal files be transmitted no later than 24 hours prior to the required proposal due date and time. Please be advised that the Government determines timeliness based solely on the date and time the proposal is received, not on the date and time the Offeror initiates transmission.

10. Proposal Submission:

    The Offeror's proposal shall be submitted electronically via email to Terricia Lloyd, Terricia.Lloyd@va.gov and Brett Schwerin, Brett.Schwerin@va.gov.

    - Subject line must include the **Solicitation Number 36C10B26Q0035, Enterprise Mammography Tracking and Reporting System**

    - Proposal must include the Offeror's Company Name, Address, contact information, and Unique Entity ID. Refer to Section E.13 for submission instructions.

11. Point of Contact Information:

    For information regarding this solicitation, contact Contract Specialist Terricia Lloyd, Terricia.Lloyd@va.gov, and Contracting Officer, Brett Schwerin, Brett.Schwerin@va.gov.

Table of Contents

SECTION B - CONTINUATION OF SF 1449 BLOCKS 6

B.1 CONTRACT ADMINISTRATION DATA 6
B.3 SOFTWARE LICENSE, MAINTENANCE AND TECHNICAL SUPPORT: 9
B.4 SHARE IT ACT 13
B.5 SCHEDULE OF SUPPLIES AND SERVICES 14
B.6 PERFORMANCE WORK STATEMENT 40

SECTION C - CONTRACT CLAUSES 119

C.1 RFO 52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (NOV 2020) 119
C.2 RFO 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998) 119
C.3 RFO 52.203-12 LIMITATION ON PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS (JUN 2020) 121
C.4 RFO 52.217-7 OPTION FOR INCREASED QUANTITY—SEPARATELY PRICED LINE ITEM (MAR 1989) 126
C.5 RFO 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999) 126
C.6 RFO 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000) 126
C.7 RFO 52.219-8 UTILIZATION OF SMALL BUSINESS CONCERNS (NOV 2025) (Deviation) 127
C.8 RFO 52.219-14 LIMITATIONS ON SUBCONTRACTING (NOV 2025) (DEVIATION) 129
C.9 RFO 52.219-16 LIQUIDATED DAMAGES-SUBCONTRACTING PLAN (NOV 2025) (Deviation) 131
C.10 RFO 52.222-90 ADDRESSING DEI DISCRIMINATION BY FEDERAL CONTRACTORS (DEVIATION APR 2026) 132
C.11 RFO 52.240-91 SECURITY PROHIBITIONS AND EXCLUSIONS (NOV 2025) (DEVIATION) 133
C.12 VAAR 852.211-76 LIQUIDATED DAMAGES – REIMBURSEMENT FOR DATA BREACH COSTS (FEB 2023) ALTERNATE I (FEB 2023) 141
C.13 VAAR 852.204-72 PERSONNEL VETTING AND CREDENTIALING (DEVIATION) (MAR 2026) 142
C.14 VAAR 852.239-76 INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY (FEB 2023) 145
C.15 MANDATORY WRITTEN DISCLOSURES 146
C.16 H CLAUSE ARTIFICIAL INTELLIGENCE IN VA CONTRACT 146
C17. BUSINESS ASSOCIATE AGREEMENT 148

SECTION D – CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS 150

D.1 LIST OF ATTACHMENTS 150
D.2 ATTACHMENT 1 – BUSINESS ASSOCIATE AGREEMENT 150
D.3 ATTACHMENT 2 – PAST PERFORMANCE QUESTIONNAIRE 150

SECTION E - SOLICITATION PROVISIONS 152

E.1 RFO 52.252-5 AUTHORIZED DEVIATIONS IN PROVISIONS (NOV 2020) 152

E.2 RFO 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998).....152
E.3 VAAR 852.252-70 SOLICITATION PROVISIONS OR CLAUSES INCORPORATED BY REFERENCE (JAN 2008).....152
E.4 RFO 52.204-5 WOMEN-OWNED BUSINESS (OTHER THAN SMALL BUSINESS) (Oct 2014).....153
E.5 RFO 52.209-5 CERTIFICATION REGARDING RESPONSIBILITY MATTERS (NOV 2025) (DEVIATION).....154
E.6 RFO 52.209-7 INFORMATION REGARDING RESPONSIBILITY MATTERS (OCT 2018).....155
E.7 RFO 52.209-11 REPRESENTATION BY CORPORATIONS REGARDING DELINQUENT TAX LIABILITY OR A FELONY CONVICTION UNDER ANY FEDERAL LAW (NOV 2025) DEVIATION.....156
E.8 RFO 52.216-1 TYPE OF CONTRACT (NOV 2025) (DEVIATION).....157
E.9 RFO 52.233-2 SERVICE OF PROTEST (NOV 2025) (DEVIATION).....157
E.10 RFO 52.227-15 REPRESENTATION OF LIMITED RIGHTS DATA AND RESTRICTED COMPUTER SOFTWARE DEC 2007.....157
E.11 RFO 52.240-90 SECURITY PROHIBITIONS AND EXCLUSIONS REPRESENTATIONS AND CERTIFICATIONS (NOV 2025) (DEVIATION).....158
E.12 VAAR 852.215-72 NOTICE OF INTENT TO RE-SOLICIT (OCT 2019).....161
E.13 NEW SOLICITATION NOTICE.....161
E.14 EVALUATION.....162
E.15 INSTRUCTIONS TO OFFEROR.....165
E.16 ARTIFICIAL INTELLIGENCE EFFORTS.....172

SECTION B - CONTINUATION OF SF 1449 BLOCKS

B.1 CONTRACT ADMINISTRATION DATA

1. Contract Administration: All contract administration matters will be handled by the following individuals:

   a. CONTRACTOR: To Be Determined, See Block 17a

   b. GOVERNMENT: Contracting Officer 36C10B, See Block 31b
   Department of Veterans Affairs
   Technology Acquisition Center
   23 Christopher Way
   Eatontown NJ 07724

2. CONTRACTOR REMITTANCE ADDRESS: All payments by the Government to the contractor will be made in accordance with:

   [X] 52.232-33, Payment by Electronic Funds Transfer—System for Award Management, or
   [] 52.232-36, Payment by Third Party

3. INVOICES: Invoices shall be submitted in arrears:
   a. Quarterly []
   b. Semi-Annually []
   c. Other [X] Monthly, after Government inspection, acceptance, and in accordance with Section B.5, Schedule of Supplies and Services

4. GOVERNMENT INVOICE ADDRESS: All Invoices from the contractor shall be submitted electronically in accordance with VAAR Clause 852.232-72 Electronic Submission of Payment Requests.

   See website at: http://www.fsc.va.gov/einvoice.asp

   ACKNOWLEDGMENT OF AMENDMENTS: The offeror acknowledges receipt of amendments to the Solicitation numbered and dated as follows:

AMENDMENT NO	DATE

5. ACCOUNTING AND APPROPRIATION DATA: To Be Provided (TBP)

6. SUBCONTRACTING PLAN - MONITORING AND COMPLIANCE
The Contractor is advised in performing contract administration functions, the CO may use the services of a support contractor(s) to assist in assessing the Contractor's compliance with the plan, including reviewing the Contractor's accomplishments in achieving the subcontracting goals in the plan. To that end, the support Contractor(s) may require access to the contractor's business records or other proprietary data to review such business records regarding the contractor's compliance with this requirement. All support contractors conducting this review on behalf of VA will be required to sign an “Information Protection and Non-Disclosure and Disclosure of Conflicts of Interest Agreement” to ensure the contractor's business records or other proprietary data reviewed or obtained in the course of assisting the CO in assessing the contractor for compliance are protected to ensure information or data is not improperly disclosed or other impropriety occurs. Furthermore, if VA determines any services the support contractor(s) will perform in assessing compliance are advisory and assistance services as defined in FAR 2.101, Definitions, the support Contractor(s) must also enter into an agreement with the contractor to protect proprietary information as required by FAR 9.505-4, obtaining access to proprietary information, paragraph (b). The Contractor is required to cooperate fully and make available any records as may be required to enable the CO to assess the contractor compliance with the subcontracting plan.

B.2 GOVERNING LAW

Federal law and regulations, including the Federal Acquisition Regulations (FAR), shall govern this Contract/Order. Commercial license agreements may be made a part of this Contract/Order but only if both parties expressly make them an addendum hereto. If the commercial license agreement is not made an addendum, it shall not apply, govern, be a part of or have any effect whatsoever on the Contract/Order; this includes, but is not limited to, any agreement embedded in the computer software (clickwrap), any agreement that is otherwise delivered with or provided to the Government with the commercial computer software or documentation (shrink wrap), or any other license agreement otherwise referred to in any document. If a commercial license agreement is made an addendum, only those provisions addressing data rights regarding the Government's use, duplication and disclosure of data (e.g., restricted computer software) are included and made a part of this Contract/Order, and only to the extent that those provisions are not duplicative or inconsistent with Federal law, Federal regulation, the incorporated FAR clauses and the provisions of this Contract/Order; those provisions in the commercial license agreement that do not address data rights regarding the Government's use, duplication and disclosure of data shall not be included or made a part of the Contract/Order. Federal law and regulation including, without limitation, the Contract Disputes Act (41 U.S.C. § 7101 et seq.), the Anti-Deficiency Act (31 U.S.C. § 1341 et seq.), the Competition in Contracting Act (41 U.S.C. § 3301 et seq.), the Prompt Payment Act (31 U.S.C. § 3901 et seq.), Contracts for Data Processing or Maintenance (38 USC § 5725), Source Code Harmonization and Reuse in Information Technology Act "SHARE IT Act" (P.L. 118-187), and FAR clauses 52.212-4, 52.227-14 shall supersede, control, and render ineffective any inconsistent, conflicting, or duplicative provision in any commercial license agreement. In the event of conflict between this clause and any provision in the Contract/Order or the commercial license agreement or elsewhere, the terms of this clause shall prevail. The Contractor shall deliver to the Government all data first produced under this Contract/Order with unlimited rights as defined by FAR 52.227-14, this includes any custom code developed for the purpose of performing under this contract. Claims of patent or copyright infringement brought against the Government as a party shall be defended by the U.S. Department of Justice (DOJ) in accordance with 28 U.S.C. § 516; at the discretion of DOJ, the Contractor may be allowed reasonable participation in the defense of the litigation. Any additional changes to the Contract/Order must be made by modification (Standard Form 30) and shall only be made by a warranted Contracting Officer. Nothing in this Contract/Order or any commercial license agreement shall be construed as a waiver of sovereign immunity.

B.3 SOFTWARE LICENSE, MAINTENANCE AND TECHNICAL SUPPORT:

1. Definitions.

   a. Licensee. The term "licensee" shall mean the U.S. Department of Veterans Affairs ("VA") and is synonymous with "Government."
   b. Licensor. The term "licensor" shall mean the Contractor having the necessary license or ownership rights to deliver license, software maintenance and support of the computer software being acquired. The term "Contractor" is the party identified in Block 17a on the SF1449. If the Contractor is a reseller and not the Licensor, the Contractor remains responsible for performance under this Contract/Order.
   c. Software. The term "software" shall mean the licensed computer software product(s) cited in the Schedule of Supplies/Services.
   d. Maintenance. The term "maintenance" is the process of enhancing and optimizing software, as well as remedying defects. It shall include all new fixes, patches, releases, updates, versions and upgrades, as further defined below.
   e. Technical Support. The term "technical support" refers to the range of services providing assistance for the software via the telephone, email, a website or otherwise.
   f. Release or Update. The term "release" or "update" are terms that refer to a revision of software that contains defect corrections, minor enhancements, or improvements of the software's functionality. This is usually designated by a change in the number to the right of the decimal point (e.g., from Version 5.3 to 5.4). An example of an update is the addition of new hardware.
   g. Version or Upgrade. The term "version" or "upgrade" are terms that refer to a revision of software that contains new or improved functionality. This is usually designated by a change in the number to the left of the decimal point (e.g., from Version 5.4 to 6).

2. Software License.
   a. Unless otherwise stated in the Schedule of Supplies/Services, the Performance Work Statement, or Product Description, the software license provided to the Government is a perpetual, nonexclusive license to use the software.
   b. The Government may use the software in a networked environment.
   c. All limitations of software usage are expressly stated in the Schedule of Supplies/Services and the Performance Work Statement/Product Description.
   d. The commercial computer software delivered under this contract may not be used, reproduced, or disclosed by the Government except as provided below or as expressly stated otherwise in this contract. The commercial computer software may be-
      i. Used or copied for use with the computer(s) for which it was acquired, including use at any Government installation or agency to which the computer(s) may be transferred.
      ii. Used or copied for use with a backup computer if any computer for which it was acquired is inoperative.
      iii. Reproduced for safekeeping (archives) or backup purposes.

iv. Modified, adapted, or combined with other computer software.
v. Disclosed to and reproduced for use by support service Contractors or their subcontractors, subject to the same restrictions set forth in this contract; and
vi. Used or copied for use with a replacement computer.

e. Unauthorized Obligations.
   i. Except as stated in paragraph (ii), when any supply or service acquired under this contract is subject to any commercial supplier agreement (as defined in 502.101) that includes any language, provision, or clause requiring the Government to pay any future fees, penalties, interest, legal costs or to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:
      1. Any such language, provision, or clause is unenforceable against the Government.
      2. Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the commercial supplier agreement. If the commercial supplier agreement is invoked through an “I agree” click box or other comparable mechanism (e.g., “click-wrap” or “browse-wrap” agreements), execution does not bind the Government or any Government authorized end user to such clause.
      3. Any such language, provision, or clause is deemed to be stricken from the commercial supplier agreement.
   ii. Paragraph (u)(1) of this clause does not apply to indemnification or any other payment by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

h. Commercial supplier agreements unenforceable clauses.
   i. This agreement is a part of a contract between the commercial supplier and the U.S. Government for the acquisition of the supply or service that necessitates a license or other similar legal instrument (including all contracts, task orders, and delivery orders under FAR 12).
   ii. End user. This agreement shall bind the ordering activity as end user but shall not operate to bind a Government employee or person acting on behalf of the Government in his or her personal capacity.
   iii. Law and disputes. This agreement is governed by Federal law. Any language purporting to subject the U.S. Government to the laws of a U.S. state, U.S. territory, district, or municipality, or a foreign nation, except where Federal law expressly provides for the application of such laws, is hereby deleted.
      1. Any language requiring dispute resolution in a specific forum or venue that is different from that prescribed by applicable Federal law is hereby deleted. Any dispute regarding the license grant or usage limitations shall be resolved in accordance with the Disputes Clause incorporated in FAR 52.212-4(d).
      2. Any language prescribing a different time period for bringing an action

than that prescribed by applicable Federal law in relation to a dispute is hereby deleted.

3. Continued performance. The supplier or licensor shall not unilaterally revoke, terminate or suspend any rights granted to the Government except as allowed by this contract. If the supplier or licensor believes the ordering activity to be in breach of the agreement, it shall pursue its rights under the Contract Disputes Act or other applicable Federal statute while continuing.
4. Arbitration; equitable or injunctive relief. In the event of a claim or dispute arising under or relating to this agreement, a binding arbitration shall not be used unless specifically authorized by agency guidance, and equitable or injunctive relief, including the award of attorney fees, costs or interest, may be awarded against the U.S. Government only when explicitly provided by statute (e.g., Prompt Payment Act or Equal Access to Justice Act).

iv. *Updating terms*. After award, the contractor may unilaterally revise commercial supplier agreement terms if they are not material. A material change is defined as:

1. Terms that change Government rights or obligations;
2. Terms that increase Government prices;
3. Terms that decrease overall level of service; or
4. Terms that limit any other Government right addressed elsewhere in this contract.
5. For revisions that will materially change the terms of the contract, the revised commercial supplier agreement must be incorporated into the contract using a bilateral modification.
6. Any agreement license terms or conditions unilaterally revised subsequent to award that are inconsistent with any material term or provision of this contract shall not be enforceable against the Government, and the Government shall not be deemed to have consented to them.

v. *No automatic renewals*. If any license or service tied to periodic payment is provided under this agreement (e.g., annual software maintenance or annual lease term), such license or service shall not renew automatically upon expiration of its current term without prior express consent by an authorized Government representative.

vi. *Indemnification*. Any clause of this agreement requiring the commercial supplier or licensor to defend or indemnify the end user is hereby amended to provide that the U.S. Department of Justice has the sole right to represent the United States in any such action, in accordance with 28 U.S.C. 516.

vii. *Audits*. Any clause of this agreement permitting the commercial supplier or licensor to audit the end user's compliance with this agreement is hereby amended as follows:

1. Discrepancies found in an audit may result in a charge by the commercial supplier or licensor to the ordering activity. Any resulting invoice must comply with the proper invoicing requirements specified in the underlying Government contract or order.
2. This charge, if disputed by the ordering activity, will be resolved in accordance with FAR 52.212-4(d); no payment obligation shall arise on the part of the ordering activity until the conclusion of the dispute process.
3. Any audit requested by the contractor will be performed at the contractor's expense, without reimbursement by the Government.

3. Software Maintenance and/or Technical Support.
   a. If the Government desires to continue software maintenance and support beyond the period of performance identified in this Contract/Order, the Government will issue a separate contract or order for maintenance and support. Conversely, if a contract or order for continuing software maintenance and technical support is not received, the Contractor is neither authorized nor permitted to renew any of the previously furnished services.
   b. The Contractor shall provide software support services, which includes periodic updates, enhancements and corrections to the software, and reasonable technical support, all of which are customarily provided by the Contractor to its commercial customers to cause the software to perform according to its specifications, documentation or demonstrated claims.
   c. Any telephone support provided by Contractor shall be at no additional cost.
   d. The Contractor shall provide all maintenance services in a timely manner in accordance with the Contractor's customary practice or as defined in the Performance Work Statement or Product Description. However, prolonged delay (exceeding two business days) in resolving software problems will be noted in the Government's various past performance records on the Contractor (e.g., www.cpars.gov).
   e. If the Government allows the maintenance and support to lapse and subsequently wishes to reinstate it, any reinstatement fee charged shall not exceed the amounts that would have been charged if the Government had not allowed the subscription to lapse.

4. Disabling Software Code.

The Government requires delivery of computer software that does not contain any code that will, upon the occurrence or the nonoccurrence of any event, disable the software. Such code includes but is not limited to a computer virus, restrictive key, node lock, time-out, or other function,

whether implemented by electronic, mechanical, or other means, which limits or hinders the use or access to any computer software based on residency on a specific hardware configuration, frequency of duration of use, or other limiting criteria. If any such disabling code is present, the Contractor agrees to indemnify the Government for all damages suffered as a result of a disabling caused by such code, and the contractor agrees to remove such code upon the Government's request at no extra cost to the Government. Inability of the Contractor to remove the disabling software code will be considered an inexcusable delay and a material breach of contract, and the Government may exercise its right to terminate for cause. In addition, the Government is permitted to remove the code as it deems appropriate and charge the Contractor for consideration for the time and effort expended in removing the code.

5. Manuals and Publications.
Upon Government request, the Contractor shall furnish the most current version of the user manual and publications for all products/services provided under this Contract/Order at no cost.

B.4 SHARE IT ACT

The Contractor shall comply with the Source Code Harmonization and Reuse in Information Technology (SHARE IT) Act, P.L. 118-187, when developing and delivering custom code first produced for the VA in the performance of this Contract/Order. The Contractor shall deliver to the Government all data first produced under this Contract/Order with unlimited rights as defined by FAR 52.227-14, to include without limitation, all custom-developed code and other key technical components of the code (including documentation, data models, schemas, metadata, architecture designs, configuration scripts, and artifacts required to develop, build, test, and deploy the code). Custom-developed code includes source code, or segregable portions of source code and all documentation created in support thereof to include source code written for a software project, product, module, plugin, script, middleware, or application programming interface.

B.5 SCHEDULE OF SUPPLIES AND SERVICES
*The directives will be removed from the resultant award.

*Offeror shall complete Section B.5, Schedule of Supplies and Services and submit it with its proposal. Note: Alterations to the line items as specified below may render proposals unacceptable. All questions must be submitted via email to the Contract Specialist, prior to the closing date and time specified in the RFP.

*Any resulting contract will be awarded on a firm-fixed-price basis as defined by Federal Acquisition Regulation Subpart 16.202, Firm-fixed-price contracts. Accordingly, the Contractor shall ensure that any and all costs associated with the Contractor's proposed application(s), software products, software solution, and/or system, shall be included in the Contractor's proposed firm-fixed price, and shall serve as the Contractor's firm-fixed price for the life of any resulting contract. No additional costs or fees relative to the Contractor's proposed application(s), software products, software solution, and/or system including, but not limited to, licensing costs and any associated licensing maintenance required for the development, delivery, integration, operation, and/or maintenance of the Contractor's proposed solution will be allowed, accepted, and/or paid by the Government.

CLIN	Description	Qty	Unit	Unit Price	Extended Price
Enterprise Mammography Tracking and Reporting System All work shall be performed in accordance with the Performance Work Statement (PWS) entitled "Enterprise Mammography Tracking & Reporting System" dated March 26, 2026, as set forth in Section B.6 herein. Period of Performance (POP): 12 months from the date of contract award. Inspection/Acceptance/FOB: Destination. Product Service Code (PSC): 6525 IFCAP: To Be Provided ARM: 200774 Point of Contact/Contracting Officers Representative: TBP					
0001	Enterprise Mammography Tracking and Reporting System Software Subscription License (Not to exceed 450,000 annual exam volume) Descriptive Data: This is a 12-month period of performance as set forth in PWS Section B.6 herein	12	Months (Mo)	$	$

CLIN	Description	Qty	Unit	Unit Price	Extended Price
0002	Installation Services inclusive of Implementation, Configuration and System Interface. Performance: 12 months after acceptance of order Description Data: Installation services for 30 locations IAW PWS Addendum C, Section 10.1, as set forth in Section B.6 herein	30	Each (Ea.)	$	$
0003	Project Management Performance: 12 months from the date of contract award. Descriptive Data: This is a 12-month effort for project management IAW PWS Section 5.1 as set forth in Section B.6 herein.	12	MO	$	$
0003AA	Contractor Project Management Plan (CPMP) Performance: Due 21 days after contract award and updated monthly thereafter throughout the PoP Descriptive Data: The contractor shall deliver the CPMP IAW PWS Section 5.1.1 as set forth in Section B.6 herein.	1	LT	Not Separately Priced (NSP)	NSP
0003AB	Monthly Progress Report Performance: Due on the fifth day of each month throughout the PoP. Descriptive Data: The contractor shall deliver the monthly progress report IAW	1	LT	NSP	NSP

CLIN	Description	Qty	Unit	Unit Price	Extended Price
	PWS Section 5.1.2 as set forth in Section B.6 herein.				
0003AC	Kick-Off Meeting Agenda Performance: Due five (5) calendar days before the kick-off meeting is held. Descriptive Data: The contractor shall deliver the kickoff meeting presentation IAW PWS Section 5.1.3 as set forth in Section B.6 herein.	1	Job (JB)	NSP	NSP
0003AD	Kick-Off Slide-Deck and Meeting Minutes Performance: Due three (3) calendar days after meeting is held. Descriptive Data: The contractor shall deliver the kick-off slide-deck and meeting minutes IAW PWS Section 5.1.3 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0004	Clinical Functionality Descriptive Data: This is a 12-month effort for clinical functionality IAW PWS Section 5.2 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0004AA	Capability Statement Performance: Due 21 days after contract award. Descriptive Data: The contractor shall deliver the capability statement IAW PWS Section 5.2.1 as set forth in Section B.6 herein.	1	LT	NSP	NSP

CLIN	Description	Qty	Unit	Unit Price	Extended Price
0004AB	System Interface and Integration Workflow Validation Checklist Performance: Due 21 days prior to each site/VISN go live milestone. Descriptive Data: The contractor shall deliver the system interface and integration workflow validation checklist IAW PWS Section 5.2.3 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0004AC	Patient Data Collection Screenshots Performance: Due 21 after contract award. Descriptive Data: The contractor shall deliver patient data collection screenshots IAW PWS Section 5.2.4 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0004AD	Completed VA Form 6550 for Patient Data Collection Tablets Performance: Due 21 after contract award. Descriptive Data: The contractor shall deliver a completed VA Form 6550 for patient data collection tablets IAW PWS Section 5.2.4 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0004AE	Functional User Communication Process	1	LT	NSP	NSP

CLIN	Description	Qty	Unit	Unit Price	Extended Price
	Performance: Due 21 days prior to each VAMC site go live. Descriptive Data: The contractor shall deliver the functional user communication process IAW PWS Section 5.2.5 as set forth in Section B.6 herein.				
0004AF	Functional MTRS Radiologist Workflow Performance: Due 21 days prior to each VAMC site go live. Descriptive Data: The contractor shall deliver the functional MTRS radiologist workflow IAW PWS Section 5.2.6 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0004AG	Patient Tracking Screenshots Performance: Due 21 days prior to each site VAMC go live. Descriptive Data: The contractor shall deliver the functional user communication process IAW PWS Section 5.2.7 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0004AH	Functional MTRS Patient Lay Summary Letters Workflow Performance: Due 21 days prior to each site VAMC go live. Descriptive Data: The contractor shall deliver the functional MTRS patient lay letters workflow IAW PWS	1	LT	NSP	NSP

CLIN	Description	Qty	Unit	Unit Price	Extended Price
	Section 5.2.8 as set forth in Section B.6 herein.				
0004AI	Compliance, Data Analytics, and Reporting Screenshots Performance: Due 21 days prior to each site VAMC go live. Descriptive Data: The contractor shall deliver the compliance, data analytics, and reporting screenshots IAW PWS Section 5.2.9 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0004AJ	Artificial Intelligence (AI) Capability Statement Performance: Due 30 days after award. Descriptive Data: The contractor shall deliver the AI capability statement IAW PWS Section 5.2.9.1 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0005	Technical Functionality Descriptive Data: The contractor shall deliver an MTRS solution with the technical functionality IAW PWS Section 5.3 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0005AA	Disaster Recovery Plan Performance: Due 21 days prior to first go live and reviewed/updated quarterly thereafter. Descriptive Data: The contractor shall deliver the disaster recovery plan IAW	1	LT	NSP	NSP

CLIN	Description	Qty	Unit	Unit Price	Extended Price
	PWS Section 5.3 as set forth in Section B.6 herein.				
0005AB	Hardware Specifications and Network Requirements Performance: Due 30 days after contract award. Descriptive Data: The contractor shall deliver the hardware specifications and network requirements IAW PWS Section 5.3 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0005AC	Manufacturer Disclosure Statement Performance: Due 30 days after contract award. Descriptive Data: The contractor shall deliver the manufacturer disclosure statement IAW PWS Section 5.3 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0005AD	Completed VA Form 6550 Performance: Due 30 days after contract award, weekly thereafter if modifications/updates are required. Descriptive Data: The contractor shall deliver the completed VA Form 6550 IAW PWS Section 5.3 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0005AE	Production and Testing System Architecture Performance: Due 60 days prior to first go live.	1	LT	NSP	NSP

CLIN	Description	Qty	Unit	Unit Price	Extended Price
	Descriptive Data: The contractor shall deliver the production and testing system architecture IAW PWS Section 5.3 as set forth in Section B.6 herein.				
0005AF	MTRS Cloud Deployment Capability Report Performance: Due 21 days after contract award. Descriptive Data: The contractor shall deliver the MTRS cloud deployment capability report IAW PWS Section 5.3 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0005AG	Enterprise MTRS Database Licenses Performance: Due 21 days prior to first go live and assessed per VAMC go live and annually thereafter. Descriptive Data: The contractor shall deliver the enterprise MTRS database licenses plan IAW PWS Section 5.3 as set forth in Section B.6 herein.	50	Each	NSP	NSP
0006	Enterprise Licenses Performance: Due 21 days prior to first go live and assessed per VAMC go live and annually thereafter. Descriptive Data: The contractor shall deliver the enterprise licenses plan IAW	1	LT	NSP	NSP

CLIN	Description	Qty	Unit	Unit Price	Extended Price
	PWS Section 5.4 as set forth in Section B.6 herein.				
0007	Data Migration Descriptive Data: The contractor shall deliver a fully functional MTRS solution to include data migration functionality IAW PWS Section 5.6 as set forth in Section B.6 herein	1	LT	NSP	NSP
0007AA	Data Migration Report Performance: Due 21 days prior to each go live. Descriptive Data: The contractor shall deliver the data migration report IAW PWS Section 5.6 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0007AB	MTRS Data in a User-Accessible Format Performance: Due 14 days prior to prior to the completion or termination of the contract. Descriptive Data: The contractor shall deliver the MTRS data in a user-accessible format IAW PWS Section 5.6 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0007AC	Administrative MTRS System and Database Credentials Performance: Due 21 days prior to prior to the first VAMC go live and reviewed quarterly. Descriptive Data: The contractor shall deliver the administrative MTRS system	1	LT	NSP	NSP

CLIN	Description	Qty	Unit	Unit Price	Extended Price
	and database credentials IAW PWS Section 5.6 as set forth in Section B.6 herein.				
0008	System Performance Descriptive Data: The contractor shall deliver a fully functional MTRS solution that adheres to the system performance as set forth in Section B.6, PWS Section 5.7 .	1	LT	NSP	NSP
0008AA	Quarterly Review Certification for System Performance Performance: Due 30 days after to the first go live and reviewed quarterly thereafter. Descriptive Data: The contractor shall deliver the quarterly review certification for system performance IAW PWS Section 5.7 as set forth in Section B.6 herein.	1	LT	NSP	NSP
00009	User and Group Functionality Descriptive Data: The contractor shall deliver a fully functional MTRS solution to include user and group functionality IAW PWS Section 5.8 as set forth in Section B.6 herein	1	LT	NSP	NSP
0009AA	User and Group Functionality Validation Report Performance: Due 21 days after each go live. Descriptive Data: The contractor shall deliver the user and group functionality validation report IAW PWS	1	LT	NSP	NSP

CLIN	Description	Qty	Unit	Unit Price	Extended Price
	Section 5.8 as set forth in Section B.6 herein.				
0010	Health Level Seven (HL7) Integration Descriptive Data: The contractor shall deliver a fully functional MTRS solution to support HL7 integration IAW PWS Section 5.9 as set forth in Section B.6 herein	1	LT	NSP	NSP
0010AA	Bi-directional HL7 Integration Validation Report Performance: Due 21 days prior to the each go live. Descriptive Data: The contractor shall deliver the bi-directional HL7 integration validation report IAW PWS Section 5.9 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0011	Digital Imaging and Communications in Medicine (DICOM) Integration Descriptive Data: The contractor fully functional MTRS solution shall be fully compliant with DICOM IAW PWS Section 5.10 as set forth in Section B.6 herein	1	LT	NSP	NSP
0011AA	DICOM Conformance Statement Performance: Due 30 days after contract award. Descriptive Data: The contractor shall deliver the DICOM conformance statement	1	LT	NSP	NSP

CLIN	Description	Qty	Unit	Unit Price	Extended Price
	IAW PWS Section 5.10 as set forth in Section B.6 herein.				
0012	Training Descriptive Data: The contractor shall provide training IAW PWS Section 5.11 as set forth in Section B.6 herein	1	LT	$	$
0012AA	Training Plan Performance: Due 21 days prior to each VAMC go live Descriptive Data: The contractor shall deliver the training plan IAW PWS Section 5.11 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0012AB	Training Attendance Records Performance: Due five (5) business days following the completion of each training event. Descriptive Data: The contractor shall deliver the training attendance records IAW PWS Section 5.11 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0012AC	Training Quick Reference Guides Performance: Due 21 days prior to each VAMC go live Descriptive Data: The contractor shall deliver the training quick reference guides IAW PWS Section 5.11 as set forth in Section B.6 herein.	1	LT	NSP	NSP

CLIN	Description	Qty	Unit	Unit Price	Extended Price
0012AD	Clinical Service Manuals Performance: Due 21 days prior to the first training date. Descriptive Data: The contractor shall deliver clinical user manuals IAW PWS Section 5.11.4 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0012AE	Technical Service Manuals Performance: Due 21 days prior to the first training date. Descriptive Data: The contractor shall deliver technical service manuals IAW PWS Section 5.11.4 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0012AF	Administrator Service Manuals Performance: Due 21 days prior to the first training date. Descriptive Data: The contractor shall deliver administrator service manuals IAW PWS Section 5.11.4 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0013	Customer Support Descriptive Data: The contractor shall provide customer support IAW PWS Section 5.12 as set forth in Section B.6 herein	1	LT	NSP	NSP
0013AA	Customer Support Status Report	1	LT	NSP	NSP

CLIN	Description	Qty	Unit	Unit Price	Extended Price
	Performance: Due semi-annually after the first go live event. Descriptive Data: The contractor shall deliver customer service support report IAW PWS Section 5.12 as set forth in Section B.6 herein.				
0013AB	Software Obsolescence Plan Performance: Due semi-annually after the first go live event. Descriptive Data: The contractor shall deliver software obsolescence plan IAW PWS Section 5.12 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0014	Electronic Healthcare Record Modernization (EHRM) Federal Electronic Health Record (FEHR) Transition Support Services Descriptive Data: The contractor shall provide EHRM FEHR transition support service IAW PWS Section 5.13 as set forth in Section B.6 herein	1	LT	NSP	NSP
0014AA	Master List of Legacy Patient Records Performance: Due 4 weeks prior to VAMC FEHR go live and updated 5 days after cutover. Descriptive Data: The contractor shall deliver master list of legacy patient records IAW PWS Section 5.13.1 as set	1	LT	NSP	NSP

CLIN	Description	Qty	Unit	Unit Price	Extended Price
	forth in Section B.6 herein.				
0014AB	Delta Patient List Performance: Due 30 days prior to VAMC FEHR go live and then within 5 days of the system cutover. Descriptive Data: The contractor shall deliver the delta patient list IAW PWS Section 5.13.1 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0014AC	VA Vendor Integration Document (VID) Performance: Due 4 months after receipt of award. Descriptive Data: The contractor shall deliver the VID IAW PWS Section 5.13.2 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0014AD	FEHR Integration and Validation Checklist Performance: Due 30 days prior to VAMC FEHR go live. Descriptive Data: The contractor shall deliver the FEHR integration and validation checklist IAW PWS Section 5.13.2 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0015	Enterprise and IT Framework Descriptive Data: The contractor shall adhere to the enterprise and IT framework general requirements as set forth in Section B.6. PWS Section 6.1 herein	1	LT	NSP	NSP

CLIN	Description	Qty	Unit	Unit Price	Extended Price
0015AA	Statement of Attestation Performance: Due 3 days after CO Authorization for use of AI and at a minimum annually thereafter (submitted prior to the exercise of any option periods), and at COR request, and upon the Contractor's proposed use of any new AI tools not contemplated at the time of last reporting. Descriptive Data: The contractor shall deliver statement of attestation IAW PWS Section 6.1.12 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0015AB	AI System/LLM Development and Operation Documentation Package Performance: Due 15 days ARO and updated Annually Thereafter as revisions require Descriptive Data: The contractor shall deliver the statement of attestation IAW PWS Section 6.1.12.1 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0015AC	Compliance Monitoring and Reporting Plan Performance: Due 30 days ARO Descriptive Data: The contractor shall deliver the statement of attestation IAW PWS Section 6.1.12.2 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0015AD	Corrective Action Plan	1	LT	NSP	NSP

CLIN	Description	Qty	Unit	Unit Price	Extended Price
	Performance: Due 10 business days after identification of any deviation of AI Principles Descriptive Data: The contractor shall deliver the statement of attestation IAW PWS Section 6.1.12.2 as set forth in Section B.6 herein.				
0015AE	AI Model/LLM Change Disclosure Performance: Due 30 days prior to implementation of change Descriptive Data: The contractor shall deliver the statement of attestation IAW PWS Section 6.1.12.3 as set forth in Section B.6 herein.	1	LT	NSP	NSP
0016	Security and Privacy Requirements Deliverable: Business Associate Agreement (BAA) Descriptive Data: The contractor shall adhere to the requirements within PWS Section 6.2 as set forth in Section B.6 herein	1	LT	NSP	NSP
0016AA	Contractor Staff Roster Performance: Due 3 days after contract award and updated throughout the PoP. Descriptive Data: The contractor shall deliver the statement of attestation IAW PWS Section 6.2.2 as set forth in Section B.6 herein.	1	LT	NSP	NSP
				Base Period Total	**$**

CLIN	Description	Qty	Unit	Unit Price	Extended Price
Option Period 1: Period of Performance: 12 Months (if exercised). This 12-month option period may be exercised by the Contracting Officer in accordance with RFO 52.217-9, “Option to Extend the Term of the Contract”. No work shall commence until a formal modification is issued by the Contracting Officer. If exercised the Period of Performance shall begin immediately upon expiration of the Base Period of Performance. Sub-Line-Item Numbers (SLINs): 0003AA trough 0003AD. 0004AA; 0004AF through 00040AI; 0005AA; 0005AG; 0007AA through 0007AC; 0008AA; 0009AA; 0010AA; 0012AA through 0012AC; 0013AA through 0013AB; 0014AA through 0014AD; 0015AA through 0015AE; and 0016AA will apply to the option period; if exercised					
1001	MTRS Enterprise Software Licenses, Maintenance and Support Service Description: The Contractor shall provide MTRS enterprise software licensing and support service IAW PWS Section 5.14 and Addendum C as set forth in Section B.6 herein.	12	Months	$	$
				Option Period 1 Total:	**$**
Option Period 2: Period of Performance: 12 Months (if exercised). This 12-month option period may be exercised by the Contracting Officer in accordance with RFO 52.217-9, “Option to Extend the Term of the Contract”. No work shall commence until a formal modification is issued by the Contracting Officer. If exercised the Period of Performance shall begin immediately upon expiration of the Option Period 1 Period of Performance. Sub-Line-Item Numbers (SLINs): 0003AA trough 0003AD. 0004AA; 0004AF through 00040AI; 0005AA; 0005AG; 0007AA through 0007AC; 0008AA; 0009AA; 0010AA; 0012AA through 0012AC; 0013AA through 0013AB; 0014AA through 0014AD; 0015AA through 0015AE; and 0016AA will apply to the option period; if exercised					
2001	MTRS Enterprise Software Licenses, Maintenance and Support Service Description: The Contractor shall provide MTRS enterprise	12	Months	$	$

CLIN	Description	Qty	Unit	Unit Price	Extended Price
	software licensing and support service IAW PWS Section 5.14 and Addendum C as set forth in Section B.6 herein.				
				Option Period 2 Total:	**$**
Option Period 3: Period of Performance: 12 Months (if exercised). This 12-month option period may be exercised by the Contracting Officer in accordance with RFO 52.217-9, “Option to Extend the Term of the Contract”. No work shall commence until a formal modification is issued by the Contracting Officer. If exercised the Period of Performance shall begin immediately upon expiration of the Option Period 2 Period of Performance. Sub-Line-Item Numbers (SLINs): 0003AA trough 0003AD. 0004AA; 0004AF through 00040AI; 0005AA; 0005AG; 0007AA through 0007AC; 0008AA; 0009AA; 0010AA; 0012AA through 0012AC; 0013AA through 0013AB; 0014AA through 0014AD; 0015AA through 0015AE; and 0016AA will apply to the option period; if exercised					
3001	MTRS Enterprise Software Licenses, Maintenance and Support Service Description: The Contractor shall provide MTRS enterprise software licensing and support service IAW PWS Section 5.14 and Addendum C as set forth in Section B.6 herein.	12	Months	$	$
				Option Period 3 Total Price:	**$**
Option Period 4: Period of Performance: 12 Months (if exercised). This 12-month option period may be exercised by the Contracting Officer in accordance with RFO 52.217-9, “Option to Extend the Term of the Contract”. No work shall commence until a formal modification is issued by the Contracting Officer. If exercised the Period of Performance shall begin immediately upon expiration of the Option Period 3 Period of Performance. Sub-Line-Item Numbers (SLINs): 0003AA trough 0003AD. 0004AA; 0004AF through 00040AI; 0005AA; 0005AG; 0007AA through 0007AC; 0008AA; 0009AA; 0010AA; 0012AA through 0012AC; 0013AA through 0013AB; 0014AA through 0014AD; 0015AA through 0015AE; and 0016AA will apply to the option period; if exercised					

CLIN	Description	Qty	Unit	Unit Price	Extended Price
4001	MTRS Enterprise Software Licenses, Maintenance and Support Service Description: The Contractor shall provide MTRS enterprise software licensing and support service IAW PWS Section 5.14 and Addendum C as set forth in Section B.6 herein.	12	Months	$	$
				Option Period 4 Total Price:	**$**
Optional Tasks: Optional Tasks 1 through 6 (CLINs 5001–5007) may be exercised individually, incrementally, or in full at any time during the period of performance at the sole discretion of the Government, via unilateral modification in accordance with RFP 52.217-7, Option for Increased Quantity – Separately Priced Line Items. No work shall commence until a formal modification to the order is issued by the Contracting Officer exercising the option Period of performance for the CLINs will be established at time of exercise.					
Optional Task 1					
5001	MTRS inclusive of implementation and Interface Services Description: The Contractor shall provide MTRS enterprise software licensing and support service IAW PWS Section 5.15.1 and Addendum C as set forth in Section B.6 herein for 58 locations. Ordered Quantity: TBD Remaining Quantity: TBD	58	each	$	$
5001AA	Post Go-Live Checklist Description: The Contractor shall deliver a post go-live checklist IAW PWS Section 5.15.1 as set forth in Section B.6 herein.	58	each	NSP	NSP

CLIN	Description	Qty	Unit	Unit Price	Extended Price
	Ordered Quantity: TBD Remaining Quantity: TBD				
5002	MTRS inclusive of implementation and Interface Services (Not to Exceed 20 each) Description: The Contractor shall provide MTRS enterprise software licensing and support service IAW PWS Section 5.15.1 as forth in Section B.6 herein. Locations will be provided if option is exercised. Ordered Quantity: TBD Remaining Quantity: TBD	20	each	$	$
5002AA	Post Go-Live Checklist (Not to Exceed 20 each) Description: The Contractor shall deliver a post go-live checklist IAW PWS Section 5.15.1 as set forth in Section B.6 herein. Ordered Quantity: TBD Remaining Quantity: TBD	20	each	NSP	NSP
Optional Task 2					
5003	Data migration (Not to Exceed 20 each) Description: The Contractor shall provide MTRS enterprise software licensing and support service IAW PWS Section 5.15.2 and Addendum C as set forth in Section B.6 herein. Quantity Ordered: TBD	20	each	$	$

CLIN	Description	Qty	Unit	Unit Price	Extended Price
	Quantity Remains: TBD				
5003AA	Data Migration Report Description: The Contractor shall deliver a data migration report IAW PWS Section 5.15.2 as set forth in Section B.6 herein. Ordered Quantity: TBD Remaining Quantity: TBD	20	each	NSP	NSP
Optional Task 3					
5004	AD HOC Training Session - Remote (Not to Exceed 20 each) Description: The Contractor shall provide MTRS enterprise software licensing and support service IAW PWS Section 5.15.3 and Addendum C as set forth in Section B.6 herein. Ordered Quantity: TBD Remaining Quantity: TBD	20	each	$	$
5004AA	Training Plan Description: The Contractor shall deliver a training plan IAW PWS Section 5.15.3 as set forth in Section B.6 herein. Ordered Quantity: TBD Remaining Quantity: TBD	20	each	NSP	NSP
5004AB	Training Attendance Records Description: The Contractor shall deliver the attendance records IAW PWS Section 5.15.3 as set forth in Section B.6 herein. Ordered Quantity: TBD	20	each	NSP	NSP

CLIN	Description	Qty	Unit	Unit Price	Extended Price
	Remaining Quantity: TBD				
Optional Task 4					
5005	AD HOC Training Session – In Person (Not to Exceed 20 each) Description: The Contractor shall provide MTRS enterprise software licensing and support service IAW PWS Section 5.15.4 and Addendum C as set forth in Section B.6 herein. Ordered Quantity: TBD Remaining Quantity: TBD	20	each	$	$
5005AA	Training Plan Description: The Contractor shall deliver a training plan IAW PWS Section 5.15.4 as set forth in Section B.6 herein. Ordered Quantity: TBD Remaining Quantity: TBD	20	each	NSP	NSP
5004AB	Training Attendance Records Description: The Contractor shall deliver the attendance records IAW PWS Section 5.15.4 as set forth in Section B.6 herein. Ordered Quantity: TBD Remaining Quantity: TBD	20	each	NSP	NSP
Optional Task 5					
5006	EHRM Go Live Support (Not to exceed 20 sites) Description: The Contractor shall provide MTRS enterprise software licensing and support service IAW PWS Section	20	each	$	$

CLIN	Description	Qty	Unit	Unit Price	Extended Price
	5.15.5 as set forth in Section B.6 herein. Ordered Quantity: TBD Remaining Quantity: TBD				
5006AA	FEHR Integration and Validation Checklist Description: The Contractor shall deliver FEHR integration and validation checklist IAW PWS Section 5.15.5 as set forth in Section B.6 herein. Ordered Quantity: TBD Remaining Quantity: TBD	20	each	NSP	NSP
5006AB	Master List of Legacy Patient Records Description: The Contractor shall deliver the master list of legacy patient records IAW PWS Section 5.15.5 as set forth in Section B.6 herein. Ordered Quantity: TBD Remaining Quantity: TBD	20	each	NSP	NSP
5006AC	Delta Patient List Description: The Contractor shall deliver the delta patient list IAW PWS Section 5.15.5 as set forth in Section B.6 herein. Ordered Quantity: TBD Remaining Quantity: TBD	20	each	NSP	NSP
Optional Task 6					
5007	AI Calculation Tool Enterprise License Description: The Contractor shall provide MTRS enterprise software licensing and support service IAW PWS Section	1	Ea.	$	$

CLIN	Description	Qty	Unit	Unit Price	Extended Price
	5.15.6 as set forth in Section B.6 herein.				
5007AA	AI Model Requirements Document (MRD) Description: The Contractor shall deliver AI MRD IAW PWS Section 5.15.6 as set forth in Section B.6 herein.	1	LT	NSP	NSP
5007AB	AI Model Development Package Description: The Contractor shall deliver AI model development package IAW PWS Section 5.15.6 as set forth in Section B.6 herein.	1	LT	NSP	NSP
5007AC	Validation and Test Report Description: The Contractor shall deliver validation and test report IAW PWS Section 5.15.6 as set forth in Section B.6 herein.	1	LT	NSP	NSP
5007AD	Technical Documentation Package Description: The Contractor shall deliver technical documentation package IAW PWS Section 5.15.6 as set forth in Section B.6 herein.	1	LT	NSP	NSP
5007AE	AI Calculation Tool Interface Description: The Contractor shall deliver AI calculation tool interface IAW PWS Section 5.15.6 as set forth in Section B.6 herein.	1	LT	NSP	NSP
5007AF	Training Package Description: The Contractor shall deliver training package	1	LT	NSP	NSP

CLIN	Description	Qty	Unit	Unit Price	Extended Price
	IAW PWS Section 5.15.6 as set forth in Section B.6 herein.				
5007AG	Maintenance and Monitoring Plan Description: The Contractor shall deliver maintenance and monitoring plan IAW PWS Section 5.15.6 as set forth in Section B.6 herein.	1	LT	NSP	NSP
				Optional Tasks Total Price	**$**
				Base Period Total Price:	$
				Optional Periods Total Price:	$
				Optional Tasks Total Price:	$
				Total Price Inclusive of All Options:	$

B.6 PERFORMANCE WORK STATEMENT

PERFORMANCE WORK STATEMENT
DEPARTMENT OF VETERANS AFFAIRS

Veteran's Health Administration
Healthcare Technology Management Program Office
National Radiology Program

Enterprise Mammography Tracking & Reporting System

Date: August 10, 2026
VA-26-00046145
PWS Version Number: 1.0

1.0 BACKGROUND

The Department of Veterans Affairs (VA), Veterans Health Administration (VHA), National Radiology Program Office strives to provide high quality, effective, and efficient solutions to those responsible for providing care to the Veterans at the point-of-care as well as throughout all the points of the Veterans' health care in an effective, timely and compassionate manner. VA depends on Clinical Information Systems (CIS) to meet mission goals.

Veterans Integrated Service Networks (VISNs) facilities across VHA may utilize various Radiology Information Systems (RIS) and Picture Archiving and Communication Systems (PACS), in addition to the Electronic Health Record (EHR). Therefore, the proposed Mammography Tracking System must be capable of integrating with these systems to ensure interoperability, accurate data exchange, and compliance with VHA standards. This integration will enable seamless workflow, reduce duplication of effort, and support comprehensive reporting and patient care management. Furthermore, VHA has substantial interface requirements between the proposed Mammography Tracking and Reporting System (MTRS), the Veterans Health Information and Systems Technology Architecture (VistA), and Federal Electronic Health Record (FEHR). This integration is critical to enable seamless workflow, reduce duplication of effort, support comprehensive reporting, and enhance patient care management.

The Veterans Health Administration (VHA) requires an Enterprise Mammography Tracking and Reporting System, software licenses, installation, technical services, and training. The MTRS will provide radiologists and clinical staff with enhanced tools to efficiently manage and monitor VHA mammography programs.

2.0 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement, the Contractor shall comply with the following:

1. "Federal Information Security Modernization Act of 2014"
2. Federal Information Processing Standards (FIPS) Publication 140-3, "Security Requirements for Cryptographic Modules", March 22, 2019
3. FIPS Pub 199. "Standards for Security Categorization of Federal Information and Information Systems," February 2004
4. FIPS Pub 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006
5. FIPS Pub 201-3, "Personal Identity Verification of Federal Employees and Contractors," January 2022
6. 10 U.S.C. § 2224, "Defense Information Assurance Program", as amended
7. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
8. Public Law 109-461 (P.L. 109-461), Veterans Benefits, Health Care, and Information Technology Act of 2006, as amended, Title IX, Information Security Matters
9. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964", as amended
10. VA Directive 0710, "Personnel Vetting Program," September 8, 2025, https://www.va.gov/vapubs/index.cfm

11. VA Handbook 0710, “Personnel Vetting Program,” September 8, 2025, https://www.va.gov/vapubs/index.cfm
12. VA Directive 6102, “Internet/Intranet Services,” August 5, 2019
13. 36 C.F.R. Part 1194 “Information and Communication Technology Standards and Guidelines,” as amended
14. Office of Management and Budget (OMB) Circular A-130, “Managing Federal Information as a Strategic Resource,” July 28, 2016
15. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”, as amended
16. NIST SP 800-66 Rev. 2, “Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,” February 2024
17. 45 C.F.R Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”); and 45 C.F.R. Parts 160 and 164, Subparts A and C, the Security Standard (“Security Rule”); as amended
18. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended
19. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
20. VA Directive 6500, “VA Cybersecurity Program,” February 24, 2021 (see VA NOTICE 24-18, dated September 27, 2024, “Update to VA Directive 6500 Cybersecurity Program”, and VA Notice 25-07, dated 3/18/25, “Amending VA Directive 6500 to incorporate M-24-15”)
21. VA Handbook 6500, “Risk Management Framework for VA Information Systems VA Information Security Program,” February 24, 2021 (see VA Notice 25-01, dated October 15, 2024, “Update to VA Handbook 6500 Risk Management Framework for VA Information Systems VA Information Security Program”, and VA Notice 25-06, dated 3/18/25, “Amending VA Directive 6500 to incorporate M-24-15”, VA Notice 25-16, dated September 15, 2025, “Amending VA Handbook 6500 to Replace Enterprise Mission Assurance Support Services Tool With Office of Information Technology Governance Risk Compliance Tool, and VA Notice 25-17, dated September 22, 2025, “Rescission Of Office Of Information Security (OIS) Deputy Assistant Secretary (DAS) Memorandum – Requirements of Proper Plan of Action and Milestones (POA&M) Completion)
22. VA Handbook 6500.2, “Management of Breaches Involving Sensitive Personal Information (SPI),” June 30, 2023
23. VA Handbook 6500.6, “Contract Security,” March 12, 2010 (see VA Notice 24-12, dated April 22, 2024, “Update to VA Handbook 6500.6, Contract Security, Appendix C VA Information and Information System Security/Privacy Language For Inclusion Into Contracts, As Appropriate”)
24. VA Handbook 6500.8, “Information System Contingency Planning,” March 25, 2025
25. VA Handbook 6500.10, “Mobile Device Security Policy,” February 15, 2018 (see VA NOTICE 25-10, dated June 9, 2025, “Use of Personally Owned Mobile Devices Policy Amendment of Department of Veterans Affairs Handbook 6500.10”, and VA Notice 25-15, dated August 22, 2025, “Update to VA Handbook 6500.10 Mobile Device Security Policy”)
26. VA Handbook 6500.11, “VA Firewall Configuration,” August 22, 2017
27. OIT Process Asset Library (PAL), OIT Process Asset Library.

28. One-VA Technical Reference Model (TRM) (reference at https://www.va.gov/trm/TRMHomePage.aspx)
29. VA Directive 6508, “Implementation of Privacy Threshold Analysis and Privacy Impact Assessment,” October 15, 2014
30. VA Directive 6510, “VA Identity, Credential and Access Management,” September 3, 2024
31. VA Handbook 6510, “VA Identity, Credential and Access Management,” September 27, 2024
32. VA Directive and Handbook 6513, “Secure External Connections,” October 12, 2017
33. VA Directive 6300, “Records and Information Management,” September 21, 2018
34. VA Handbook, 6300.1, “Records Management Procedures,“ March 24, 2010
35. NIST SP 800-37 Rev 2, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,” December 2018
36. NIST SP 800-53 Rev. 5, “Security and Privacy Controls for Federal Information Systems and Organizations,” September 23, 2020 (includes updates as of 12/10/2020)
37. VA Directive 0735, “Homeland Security Presidential Directive 12 (HSPD-12) Program,” October 26, 2015
38. VA Handbook 0735, “Homeland Security Presidential Directive 12 (HSPD-12) Program,” March 24, 2014
39. OMB Memorandum 05-24, “Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors,” August 5, 2005
40. OMB Memorandum M-19-17, “Enabling Mission Delivery Through Improved Identity, Credential, and Access Management,” May 21, 2019
41. OMB Memorandum, “Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation,” May 23, 2008
42. Federal Identity, Credential, and Access Management (FICAM) Architecture, June 30, 2023 (FICAM Architecture (idmanagement.gov))
43. NIST SP 800-116 Rev 1, “Guidelines for the Use of Personal Identity Verification (PIV) Credentials in Facility Access,“ June 2018
44. NIST SP 800-63 Rev 4, 800-63A-4, 800-63B-4, 800-63C-4, “Digital Identity Guidelines,” August 1, 2025
45. NIST SP 800-157, “Guidelines for Derived PIV Credentials,” December 2014
46. VA Memorandum, VAIQ #7100147, “Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12),” April 29, 2011 (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
47. IAM Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, PIV/IAM (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
48. VA Memorandum “Personal Identity Verification (PIV) Logical Access Policy Clarification,” July 17, 2019, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4896
49. Trusted Internet Connections (TIC) 3.0 Core Guidance Documents, https://www.cisa.gov/publication/tic-30-core-guidance-documents
50. OMB Memorandum M-19-26, “Update to the Trusted Internet Connections (TIC) Initiative,” September 12, 2019

51. OMB Memorandum M-08-23, “Securing the Federal Government’s Domain Name System Infrastructure,” August 22, 2008
52. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (P.L. 110–140), December 19, 2007
53. Section 104 of the Energy Policy Act of 2005, (P.L. 109–58), August 8, 2005
54. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
55. Executive Order 14148, “Initial Rescissions of Harmful Executive Orders and Actions,” dated January 20, 2025
56. VA Directive 0057, “VA Environmental Management Program,” October 25, 2022
57. OIS VAIQ #7424808 Memorandum, “Remote Access,” January 15, 2014, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
58. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
59. “Veteran Focused Integration Process (VIP) Guide 4.0,” March 2021, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371
60. VA Memorandum “Proper Use of Email and Other Messaging Services,” January 2, 2018, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
61. “Product Line Management Transformation Playbook” version 3.1, August 2023, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4946
62. NIST SP 500-267B Revision 1, “USGv6 Profile,” November 2020
63. OMB Memorandum M-21-07, “Completing the Transition to Internet Protocol Version 6 (IPv6),” November 19, 2020
64. Social Security Number (SSN) Fraud Prevention Act of 2017
65. Section 240 of the Consolidated Appropriations Act (CAA) 2018, March 23, 2018
66. C.F.R Title 15 Part 7, “Securing the Information and Communications Technology and Services (ICTS) Supply Chain”, as amended
67. Executive Order 14028, “Executive Order on Improving the Nation's Cybersecurity,” May 12, 2021, https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2025/01/16/executive-order-on-strengthening-and-promoting-innovation-in-the-nations-cybersecurity/
68. OMB Memorandum M-22-09, “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles”, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.
69. NIST SP 800-52 Revision 2, “Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
70. OMB M-26-05, “Adopting a Risk-based Approach to Software and Hardware Security,” January 23, 2026
71. OMB M-21-31, “Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents,” August 27, 2021
72. NIST SP 800-88 Revision 1 “Guidelines for Media Sanitization,” December 2014
73. CISA Binding Operational Directive (BOD) 19-02: “Vulnerability Remediation Requirements of Internet-Accessible Systems,” April 29, 2019, BOD 19-02: Vulnerability Remediation Requirements for Internet-Accessible Systems | CISA
74. CISA BOD 22-01: “Reducing the Significant Risk of Known Exploited Vulnerabilities,” November 3, 2021, BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities | CISA
75. CISA BOD 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks.” Cybersecurity & Infrastructure Security Agency (CISA), BOD

23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks | CISA

76. VA Directive 6550, Pre-Procurement Assessment and Implementation of Medical Devices/Systems, June 03, 2019
77. VA Memorandum, "VA Security Controls," January 17, 2025, https://www.voa.va.gov/DocumentView.aspx?DocumentID=5010
78. E.O. 13960, "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government," December 3, 2020
79. E.O. 14319, "Preventing Woke AI in the Federal Government," July 23, 2025
80. OMB Memorandum M-25-21, "Accelerating Federal Use of AI through Innovation, Governance, and Public Trust," April 3, 2025
81. OMB Memorandum M-25-22, "Driving Efficient Acquisition of Artificial Intelligence in Government," April 3, 2025
82. OMB Memorandum M-26-04, "Increasing Public Trust in Artificial Intelligence (AI) Through Unbiased AI Principles," December 11, 2025

3.0 SCOPE OF WORK

The Contractor must provide an enterprise-level MTRS that delivers the functionality described herein to all VHA Facilities offering in-house mammography services, including the National Teleradiology Program, and provides oversight and analytics capabilities for the National Radiology Program (NRP).

The Contractor shall provide a scalable solution to support future in-house mammography programs and shall be implemented through a phased deployment approach to maximize organizational learning and optimize project management resources. During the base year, the Contractor shall deploy the solution to an initial 30 sites. The Contractor shall complete foundational infrastructure requirements, to include configuring and activating the servers and enterprise risk assessment, in conjunction with EMTRS deployment at each site. After successful deployment, the system shall be rolled out to the remaining 58 sites. There may be a futuristic need for adding a quantity of up to 20 additional sites within the contract lifecycle. The Contractor shall coordinate each phase of the project with the Primary Contracting Officer's Representative (COR) or point of contact. Detailed discussions regarding phase activities shall occur with the Contractor during the pre-work orientation.

The Contractor shall provide an enterprise-level software license and installation services for a Mammography Tracking and Reporting System. The Contractor shall also provide training, system maintenance, and data migration services for each facility. Upon completion of installation, testing, and training, VHA shall have a national, state-of-the-art Mammography Tracking System.

The contractor shall account for the following VA Mammography Program characteristics:

- A national benchmark of 450,000 exams for all 88 sites.
- Base year 30 site implementation exam volume is estimated at 175,000 exams.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The Period of Performance (PoP) shall be 12 months from the date of award, with four 12-month option periods, and six Optional Tasks that may be exercised anytime during performance. The overall Period of Performance, including the exercise of any options, shall not exceed 60 months.

Any work at the Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO). There may be instances during deployment or system upgrades where work may need to occur on Weekends, Holidays, Evening, or Nights (WHEN hours). In those instances, the work schedule needs to occur with express permission from the COR or local Point of Contact (POC) in writing.

There are 11 Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

Under current definitions, five are set by date:

New Year's Day	January 1
Juneteenth	June 19
Independence Day	July 4
Veterans Day	November 11
Christmas Day	December 25

If any of the above falls on a Saturday, then Friday shall be observed as a holiday. Similarly, if one falls on a Sunday, then Monday shall be observed as a holiday.

The other six are set by a day of the week and month:

Martin Luther King's Birthday	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Thanksgiving	Fourth Thursday in November

4.1.1 PLACE OF PERFORMANCE

Tasks under this PWS shall be performed in VA facilities located in 88 in-house Mammography Programs across 56 VAMC/Healthcare Systems in addition to the National Teleradiology Program (NTP) and National Radiology Program Office. Work may be performed at remote locations with prior concurrence from the Contracting Officer’s Representative (COR). Refer to Addendum C for the complete listing of the 30 facilities included in the base period and the 58 facilities identified for the optional task.

VA reserves the right to update Addendum C to add locations as required to define future requirements.

4.1.2 TRAVEL

The Government anticipates travel under this effort for task execution, go-live support, and training throughout the PoP. The Contractor shall include the travel price as a firm-fixed-price line items (e.g., site preparation support, implementation support, system training).

The total estimated number of trips in support of site prep support, implementation support, training and other related efforts for this effort is 58 trips estimated at 5-days each. The Government may require additional ad hoc trips for system upgrades or ad hoc training.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall deliver a fully functional MTRS in accordance with Sections 5.1 through 5.13 of the PWS. The Contractor shall deliver a solution that provides a single

service account manager for VHA. The solution shall incorporate comprehensive project management services, including but not limited to:

1. Software, network, and implementation planning
2. Timeline
3. National-level installation with regional and site-level permissions.
4. Contracting logistics for system support and sustainment planning

Deliverable:
Fully functioning MTRS

The contractor shall perform the following:

5.1 PROJECT MANAGEMENT

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall deliver a Contractor Project Management Plan (CPMP) that defines the Contractor's approach, timeline, and tools for a fully functioning Mammography Tracking and Reporting System (MTRS). The CPMP shall include both narrative and graphic formats displaying the schedule, milestones, risks, and resource allocations, as well as planned, routine, and ad hoc procedures for data collection and reporting as specified in the PWS. The initial baseline CPMP shall be reviewed and approved by VA and updated in accordance with Section B of the contract. The Contractor shall maintain and update the VA PM-approved CPMP throughout the PoP. The Contractor shall provide a dedicated Project Management and Installation Support team for the planning, implementation, sustainment, and contracting phases of the project. The Contractor shall provide a software obsolesce plan, including advance notification of any end of life or end of support events. Notifications shall be provided at a minimum of six-months prior to the end of support date or as soon as the Contractor becomes aware, whichever is earlier.

Deliverable:
A. Contractor Project Management Plan

5.1.2 REPORTING REQUIREMENTS

The Contractor shall provide the COR with Monthly Progress Reports during the implementation phase in electronic form (Microsoft Word and Project formats). The Monthly Progress Reports shall include detailed instructions and explanations for each required data element, to ensure that data is accurate and consistent. The report shall reflect data as of the last day of the preceding month. The Contractor shall include system support updates in the monthly progress report. At a minimum, the report shall identify all system support activities performed, issues resolved, enhancements implemented, outstanding support tickets, and any risks or dependencies affecting system performance or availability.

The Monthly Progress Reports shall include work completed during the reporting period, work planned for the next period, and identify any issues encountered, along with the

resolution actions taken. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving the issue. The report shall include an itemized list of all Information and Communication Technology (ICT) deliverables and the current Section 508 conformance status. The Contractor shall monitor performance in accordance with the CPMP and report any deviations. The Contractor shall maintain regular communication with VA to ensure transparency regarding any issues that arise and to prevent escalation of unresolved matters.

Deliverable:
A. Monthly Progress Report

5.1.3 KICK-OFF MEETING

The Contractor shall establish and hold a technical kick-off meeting no later than ten calendar days after contract award, via MS Teams or conference call. The Contractor shall present the details of its intended approach, work plan, and project schedule. The Contractor shall specify the date and provide all attendees with an electronic copy of the agenda at least five calendar days before the meeting. The Contractor shall invite the CO, Contract Specialist, COR, and the VA PM. The Contractor shall provide Meeting Minutes and slide-deck to all attendees within three calendar days after the meeting.

Deliverables:
A. Kick-Off Meeting Agenda
B. Kick-Off Meeting Slide-Deck and Meeting Minutes.

5.2 CLINICAL FUNCTIONALITY

The Contractor's fully functional MTRS solution shall support comprehensive clinical operations, including breast examination management, system and interface integration, patient data collection, user communication, radiologist workflow, patient tracking, summary letter generation, compliance and analytics reporting, and records management. The MTRS shall include the following capabilities:

5.2.1 BASELINE CLINICAL FUNCTIONALITY

The Contractor shall provide a capability statement for the MTRS solution that supports reporting for the following breast examinations:

1. Magnetic Resonance Imaging (MRI)
2. Ultrasound
3. Mammography
4. Contrast Enhanced Mammography (CEM)
5. Various image guided breast biopsies & tumor localizations
6. Molecular Breast Imaging (MBI)

Deliverable:
A. Capability Statement

5.2.2 MAMMOGRAPHY TRACKING AND REPORTING SYSTEM ADMINISTRATION

The Contractor shall provide an MTRS solution with the following system functionality:

A. The Contractor shall provide a solution that enables reports customization at the system administrator level.

B. The system shall allow role-based access control for reports and analytics, ensuring that access can be restricted to specific user groups through routine system administration.

5.2.3 SYSTEM INTERFACES AND SYSTEM INTEGRATION

The Contractor shall deliver a MTRS solution with the following functionality:

A. Auto-updates patient demographics upon registration.

B. Solution that receives demographic data from VistA and FEHR via Health Level 7 (HL7).

C. Receive multiple Patient identifiers including Electronic Data Interchange Personal Identifier (EDIPI) and social security number (SSN).

D. Ability to transfer patients between facilities and EHR systems.

E. Bi-directionally integrates with both VistA/CPRS and FEHR for admit discharge transfer (ADT) and transmission of reports and lay letters.

F. Transmits both diagnostic breast imaging reporting and data system (BI-RADS) Codes both discreetly AND within the textual HL7 report message to the FEHR and VistA/CPRS.

G. Integrate with third (3rd) party artificial intelligence (AI) software systems to enhance diagnostic workflow support.

H. The total entry points for the MTRS solution shall include:

    a. PowerScribe API integration
    b. HL7 notifications for ADT inbounds info
    c. HL7 outbounds for reports
    d. encapsulated PDF reports outbound
    e. DICOM/HL7 for lay letter outbounds
    f. Active connections to both VistA/CPRS and Federal EHR through a DAS SPOE middleware integration point
    g. Connection with AI solutions (such as density) should be included in the proposal with a future potential to connect with all 88 sites

The Contractor shall deliver a system interface and integration workflow validation checklist that demonstrates the functionality in Sections A through G.

Deliverable:
System Interface and Integration Workflow Validation Checklist

5.2.4 Patient Data Collection

The Contractor proposed solution shall:

A. Deliver a solution that includes patient/family history questionnaire.

B. Provides multiple ways to gather patient history.

C. Summary of proposed tablet-based solutions capable of importing intake information directly into the system.

D. Complete a separate VA form 6550 for a tablet solution to properly assess capability to meet VA's networking and security requirements.

E. Includes Breast Cancer Risk Assessment.

   1. Breast cancer risk modules, including the Tyrer Cuzick risk management module.
   2. Turns on and off the different risk management modules.

The Contractor shall deliver screenshot(s) showing patient history and breast cancer risk assessment features, as well as VA Form 6550 filled out for any tablet offerings for patient information intake functionality. The documentation must be sufficiently detailed to verify the results and support Government review.

Deliverables:
A. Patient Data Collection Screenshot(s).
B. Completed VA Form 6550 for Patient Data Collection Tablets

5.2.5 USER COMMUNICATION

The Contractor's MTRS solution shall provide a functional user communication process that enables Radiologists and Technologists to enter or delete comments within the system and annotate the patient history form with clinical findings such as scars, moles, or other relevant observations.

Deliverable:
A. Functional User Communication Process

5.2.6 RADIOLOGIST WORKFLOW

The Contractor's fully functional MTRS radiologist workflow solution shall:

A. Provide vendor-driven radiologist workflows incorporating application programming interface (API) functionality with PACS and voice dictation systems.

B. Integrate with the VA's voice recognition system(s) at the time of implementation (currently PowerScribe 360 or PowerScribe One 2019).

C. Integrate with multiple instances (20+) of VA's current voice recognition system(s) simultaneously (currently PowerScribe 360 or PowerScribe One 2019).

D. Deliver reporting template capabilities, mammography screening, and diagnostic reports.

Deliverable:
A. Functional MTRS Radiologist Workflow

5.2.7 PATIENT TRACKING

The Contractor's fully functional MTRS solution shall:

A. Allow for identification of women due for a screening mammogram.

B. Allow for identification of patients waiting for pathology results.

C. Support comprehensive patient tracking from mammogram screening through tissue diagnosis. The solution shall also include the ability to demonstrate this functionality through screenshots displaying sample worklists and patient tracking workflows. The Contractor shall deliver patient tracking screenshots.

Deliverable:
A. Patient Tracking Screenshots

5.2.8 PATIENT LAY SUMMARY LETTERS

The Contractor's fully functional MTRS solution shall:

A. Deliver a solution that includes a workflow for sending results letters to the patients with different triggers to initiate the letter.

B. Allow for some nationally standardized portions of the Results letters that cannot be changed locally, while still allowing some aspects of the results letter to be customized by the facility.

C. Provide the ability to create a customizable patient lay summary letter for both sexes to incorporate Mammography Quality Standards Act (MQSA) guidelines.

D. Allow approved VA personnel to edit the patient lay summary letters with no or minimal support from the Contractor.

E. Include a workflow that seamlessly sends the patient lay summary letters to VISTA/CPRS & FEHR in association with the final report or images.

F. At a minimum, have the capability to print patient lay summary letters in English and Spanish.

Deliverable:
A. Functional MTRS Patient Lay Letters Workflow

5.2.9 COMPLIANCE, DATA ANALYTICS, AND REPORTING

The Contractor's fully functional MTRS solution shall:

A. Comply with the FDA regulations, American College of Radiology (ACR) accreditation, and VHA data reporting requirements:

   1. FDA Mammography Audit
   2. Includes all reports included in the audit and monitoring section of the ACR BI-RADS v2025 manual.

B. The Contractor shall have the ability to continuously meet and maintain any updated ACR BIRADS manual during the life of this contract.

C. The capability to analyze data and develop customized reports for Veteran-specific data.

D. Ability to document the Radiologist's continuing experience through both primary and secondary reads.

E. Ability to analyze data, document the number of mammograms a Radiologist has reviewed to maintain their credentials.

F. Analyze data and provide reports with clearly identified titles and scope of data (e.g., entire facility, single radiologist, entire VISN, entire VA).

G. Ability to restrict access based on assigned roles, ensuring facility-level users see only their facility's data, while designated personnel may access VISN- or VHA-level reports.

H. Allow VA to be compliant with the FDA's Enhancing Quality Using the Inspection Program (EQUIP) components.

I. The capability to automatically capture the density language and document in the MTRS.

The Contractor shall provide compliance, data analytics, and reporting screenshots illustrating the system's functionalities.

Deliverable:
A. Compliance, Data Analytics, and Reporting Screenshots

5.2.9.1 ARTIFICIAL INTELLIGENCE CALCULATION TOOL

The contractor shall deliver an Artificial Intelligence (AI) capability statement that describes their ability to implement an AI calculation tool for a 5-year risk score in alignment with the most recent NCCN guidelines for breast cancer screening and diagnosis. The capability statement shall also include the Contractor's ability to:

1. Design, develop, validate, and deliver an AI enabled risk calculation tool capable of generating individualized 5-year risk predictions based on predefined clinical, demographic, or operational data inputs.
2. Implement an AI calculation tool enterprise license.
3. Integrate an AI/ML model capable of producing a 5-year risk score with documented methodology.
4. Ensure the model includes explainability features to support decision making and operational transparency.
5. Perform internal validation (e.g., cross validation) and provide calibration metrics to demonstrate model accuracy and reliability. The Contractor shall conduct external validation using an independent dataset provided either by the Government or by the Contractor with Government approval.
6. Provide documentation detailing the model's data sources, assumptions, limitations, and governance controls. The Contractor shall identify and mitigate any model bias and provide testing results demonstrating equitable performance across demographic groups.
7. Provide an interface (API, dashboard, or module) that allows Government users to access the 5-year risk output within the enterprise MTRS software. The Contractor shall ensure compatibility with Government systems as specified in the Task Order.
8. Provide user training materials and conduct knowledge transfer sessions for Government personnel.
9. Provide ongoing model monitoring and updates, including retraining, recalibration, and performance reporting at intervals specified by the Government.

Deliverable:
A. AI Capability statement

5.2.10 RECORDS MANAGEMENT

The Contractor's fully functional MTRS solution shall enable access to patient records for forms printing and information upload when the system is unavailable at the time of the exam.

5.3 TECHNICAL FUNCTIONALITY

The Contractor's fully functional MTS solution shall be delivered at an enterprise level. The solution shall be managed according to assigned roles at the facility, VISN, and/or VHA level.

A. The solution must be non-developmental (i.e., commercially available, in current production as of the date this offer is submitted). The Contractor shall:

    1. Specify the proposed server and client software versions, as well as any web-based client software capabilities.
    2. List the actual major and minor releases, including dates, for the past two years for the proposed Mammography Tracking and Reporting System.
    3. List any third (3rd) party software components included in the proposed MTRS and whether the cost is included in the proposed licensing models.

        a. Describe the business and technical agreements that are in place to ensure ongoing support and development.
        b. List all database(s) that are used for the proposed Mammography Tracking and Reporting System.

B. The Contractor shall provide a comprehensive Disaster Recovery Plan to ensure data integrity and restoration including internal MTRS backup capabilities, and the ability of the software to support enterprise backup solutions such as Commvault. The plan shall include:

    1. A process for performing automated system backups.
    2. A process for restoring system backups.
    3. A summary of 3rd party enterprise solutions/agents that the MTRS system supports (For example, Commvault)

C. The proposed MTRS Solution shall include a test system that replicates the production environment. The Contractor shall deliver system architecture documentation for both production and test environments. The Production and Testing System Architecture document shall describe all architectural components, configurations, integrations, and dependencies required to support the enterprise MTRS solution in each environment.

    1. The test system shall validate software upgrades, new modalities, interfaces, and integrated applications.
    2. The physical location for the test system will be at the discretion of VA.
    3. The VA will provide the test environment and servers for network and interface testing.

D. The Contractor shall provide recommended Hardware Specifications and Network Requirements for the following:

    1. Main production system
    2. Workstation, including specifications regarding graphic cards and monitors

3. Test server
4. Client Software

E. The Contractor shall provide a completed copy of the Manufacturer Disclosure Statement for Medical Device Security (MDS2).

F. The Contractor shall provide a completed copy of the VA Form 6550.

G. The Contractor's solution shall provide patient context exchange and synchronization between PACS/Dictation applications and mammography tracking software solution.

H. The Contractor's solution shall be able to work across all time zones where VHA may deploy the solution.

I. The contract shall provide an MTRS Cloud Deployment Capability Report summarizing FEDRAMP status for cloud deployment, and whether the proposed MTRS solution can be implemented in the VA Enterprise Cloud Environment (VAEC). For each site the technical environment will be individual workstation level connections to the national instance of the MTRS solution.

J. Diagnostic Mammography imaging storage will be handled by the PACS solutions. Diagnostic mammography images will not be stored in the MTRS solution.

    a. Non-imaging mammography data will be stored in the MTRS solution.
    b. For storage volume considerations, reference the exam volumes outlined in section 3.0.

The Contractor shall deliver all software licenses required to support the full functionality of the enterprise MTRS solution. Deliverables shall include all database products (e.g. SQL, Oracle), components, and associated licensing necessary for the MTRS application, data storage, data processing, reporting modules, and any perpetual licenses supporting database infrastructure.

Deliverables:
A. Disaster Recovery Plan
B. Hardware Specifications and Network Requirements
C. Manufacturer Disclosure Statement
D. Completed VA Form 6550
E. Production and Testing System Architecture
F. MTRS Cloud Deployment Capability Report
G. Enterprise MTRS Database Licenses

5.4 ENTERPRISE LICENSES

The Contractor shall provide an Enterprise-Level Software License that permits unlimited concurrent user access. A list of applicable sites can be found herein at Addendum C.

Deliverable
A. Enterprise Software Licenses

5.5 IMAGING ORDERS AND REPORTS

The Contractor's fully functional MTRS solution shall be capable of entering imaging orders into the VistA Radiology Package or Oracle Health Millenium OpenLink. Each location may have up to two (2) separate VistA HL7 feeds instances, and one (1) national instance for OH OpenLink HL7 feed within VHA. The MTS solution must support an unlimited number of HL7 interfaces for ingestion.

5.6 DATA MIGRATION

The Contractor's fully functional MTRS solution shall include Data Migration and Data Migration Reports formatting of studies from the current Mammography information systems for all prior studies in advance of each respective VAMC go-live. The data migration must include, at a minimum, the last five (5) years of data.

VHA currently uses the following systems:

System	Number of Sites
MagView	12
Volpara/Patient Hub	67
Volpara/MRS	4
Unknown	5

Prior to contract completion or termination, the Contractor shall deliver all MTS data in a User-Accessible Format, assume full responsibility for project management and associated costs. Furthermore, the Contractor shall provide the Department of Veterans Affairs with all administrative system and database credentials required for system management and sustainment.

The Contractor shall conduct data migration services and provide a report for all VHA sites/legacy MTRS systems as listed in Addendum C.

The Contractor shall provide a comprehensive list of all administrative MTRS System and Database Credentials available at the time of go-live.

Deliverables:
A. Data Migration Report
B. MTRS data in a User-Accessible Format
C. Administrative MTRS System and Database Credentials

5.7 SYSTEM PERFORMANCE

The Contractor's fully functional MTRS solution shall include a minimum uptime guarantee of 99%.

1. System events caused by the VA network side, where the vendor is not at fault, will not be counted towards the count of system downtime hours.

2. Uptime is calculated based off the following:

$$\left(\frac{Hours\ of\ Coverage - Hours\ Down}{Hours\ of\ Coverage}\right) \times 100 = Uptime$$

   a. Hours of coverage in the above equation excludes hours for preventative and scheduled maintenance of the system.

   b. The MTRS system is classified as "down" when the system is unavailable for clinical use due to an unplanned event.

3. Planned Maintenance shall be planned outside of normal business hours, unless specified otherwise by the VA in writing.

4. The Contractor shall review the VA provided quarterly uptime log and performance report, verify compliance with a minimum system availability threshold of 99%, and provide a Quarterly Review Certification.

The Contractor's solution shall communicate the capability to remain active during database maintenance jobs or other server activities.

Deliverable:
A. Quarterly Review Certification for System Performance

5.8 USER AND GROUP FUNCTIONALITY

The Contractor's fully functional MTRS solution shall:

A. Support application authentication using Single Sign-On (SSO) or Lightweight Directory Access Protocol (LDAP) via personal identity verification (PIV) cards.

B. Provide the capability to develop user groups with distinct privileges/permissions. The permissions for the default user groups shall be capable of being modified by a designated VA system administrator.

C. Allow staff to see patients nationwide and input information at their local facility without creating a duplicate patient. Staff shall not be capable of printing letters for other stations.

D. Allow customizable administrative and clinical access.

The Contractor shall ensure all user and group functionality is fully validated and confirmed operational prior to each VAMC go-live. The Contractor shall deliver a User and Group Functionality Validation Report which includes documented test results demonstrating correct role assignments, access permissions, authentication behavior, and successful execution of all required user and group functions without error. Validation shall be complete upon Government acceptance and concurrence.

Deliverable:
A. User and Group Functionality Validation Report

5.9 HEALTH LEVEL SEVEN (HL7) INTEGRATION

The Contractor's fully functional MTRS solution shall support bi-directional HL7 integration with VistA and FEHR. The Contractor shall ensure the solution complies with and successfully completes the VA qualification process for both VistA and FEHR HL7 interfaces to guarantee interoperability and adherence to VA standards.

The contractor shall deliver a report confirming validation for the Bi-Directional HL7 Integration with both VistA and FEHR. The report shall be updated upon go-live at each site.

Deliverable:
A. Bi-Directional HL7 Integration Validation Report

5.10 DIGITAL IMAGING AND COMMUNICATIONS IN MEDICINE (DICOM) INTEGRATION

The Contractor's fully functional MTRS solution shall be fully compliant with the Digital Imaging and Communications in Medicine (DICOM) standard for features and workflows involving the storage, retrieval, and transmission of medical images and associated data in accordance with DICOM protocols to ensure interoperability with VA imaging systems, Picture Archiving and Communication Systems (PACS), and other healthcare applications.

The Contractor shall deliver a DICOM Conformance Statement detailing all supported DICOM services, modalities, message types, and implementation specifications no later than 30 days prior to go-live.

Deliverable:
DICOM Conformance Statement

5.11 TRAINING

The Contractor's fully functional MTRS solution shall include clinical, system administrator, and Healthcare Technology Management (HTM) training as specified below.

The Contractor shall provide Training Plan, Training Attendance Records, and Training Quick Reference Guides for all personnel who participate in required training activities. All training documentation shall be delivered to the Government in a format acceptable within 5 business days after training completion.

Deliverables:
A. Training Plan
B. Training Attendance Records
C. Training Quick Reference Guides

5.11.1 CLINICAL-USER TRAINING

A. Clinical users training shall include, but not limited to:

1. Radiologic Technologist
2. Radiologist
3. Breast imaging nurse navigators/coordinators
4. System-wide clinical administrators
5. Program support assistant/medical support assistant (MSA)

B. Upon completion of training, clinical users must be able to successfully utilize all available features with minimal or no assistance from a VA or Contractor super user.

5.11.2 SYSTEM ADMINISTRATOR TRAINING

The Contractor shall provide power-user and system administrator training for operational support of the MTRS solution.
Upon completion of training, the System administrator must be able to:

1. Act as the local super user for the clinical users
2. Act as the local trainer for the clinical users
3. Resolve the top ten most common user questions
4. Create and manage user accounts
5. Install and configure the client application for a new user
6. Monitor system utilization
7. Manage other day-to-day tasks required for the system

5.11.3 HEALTHCARE TECHNOLOGY MANAGEMENT

The Contractor shall provide biomedical engineer training for implementation and operational support for MTRS solution.

Upon completion of training the biomedical engineers shall:

1. Act as the local system expert
2. Understand the functions of each system's components
3. Be able to start the system, including the different services that make up the MTRS solution
4. Locate and review application logs
5. Install and configure the client application for a new user
6. Be able to conduct, at minimum, basic troubleshooting
7. Understand the procedure for a "graceful" system shutdown/reboot
8. Understand disaster recovery recommendations and features
9. Understand contingency operations actions and steps for VAMCs if the system were to go down or be in a compromised state.

5.11.4 SERVICE MANUALS

The contractor shall provide Clinical User, Technical, and Administrator Service Manuals for the MTRS in an electronic format.

Deliverable:
A. Clinical User Service Manuals
B. Technical Service Manuals
C. Administrator Service Manuals

5.12 CUSTOMER SUPPORT

The contractor shall provide MTRS clinical and technical support as follows:

A. Software obsolescence, major upgrades, revisions, patches and fixes for the contract period. The Contractor shall deliver a Software Obsolesce Plan, which shall be included in the CPMP as specified in Section 5.1.1 of this PWS.

B. The contractor shall provide support based on the severity level of the event as outlined in the table below. Business hours are defined as 7 am ET to 6 pm Hawaii standard time due to the national enterprise system having to account for business hours across time zones with VA mammography programs.

Severity Level	Description	Initial Response Target	Target Restoration Time
Critical	The software is down; no workaround is immediately available.	90 minutes	4 hours
High	Important software features are unavailable to multiple users; no acceptable workaround.	4 business hours	1 business day
Moderate	Software features are unavailable to multiple users; a workaround exists and most software functions are still useable.	12 business hours	5 business days

Severity Level	Description	Initial Response Target	Target Restoration Time
Low	Minor problem or question that does not affect software functionality.	24 business hours	Target restoration as agreed to between VA and the contractor on a case-by-case basis. Communication and updates need to occur on a regular basis until the case is resolved.

C. The Contractor shall provide remote technical and clinical applications support.

D. The contractor shall support ongoing workflow and integration changes as VA incrementally adds additional sites as requested.

E. Contractors with an existing approved Memorandum of Understanding Information Security Agreement (MOU/ISA) shall provide remote system support and comply with all requirements written in the MOU/ISA.

F. The contractor shall provide technical expertise regarding system patching and updates including but not limited to operating system (OS) patches, application updates, database updates, and system vulnerabilities.

The Contractor must submit a Customer Support Status Report. This report shall be included in the monthly report as specified in Section 5.1.2 of this PWS

Deliverables:
A. Customer Support Status Report
B. Software Obsolescence Plan

5.13 ELECTRONIC HEALTHCARE RECORD MODERNIZATION (EHRM) FEHR TRANSITION SUPPORT SERVICES

5.13.1 LEGACY DATABASE BULK EDIT FOR ELECTRONIC DATA INTERCHANGE PERSONAL IDENTIFIER & SOCIAL SECURITY NUMBER CONVERSION

The Contractor shall provide support services for a one-time patient identifier conversion and merge process within the legacy Mammography Tracking System (MTS) database. This effort shall include move/downgrade primary Medical Record Number (MRN) (Patient Identifier) that is currently Social Security Number (SSN) to a secondary Patient Identifier if possible and insert corresponding Electronic Data Interchange Personal Identifier (EDIPI) (New Patient Identifier) into the primary MRN field or status.

The Contractor shall compile and deliver a Master List of Legacy Patient Records, including SSNs and available attributes (e.g., Last Name, First Name,

Date of Birth, Sex), in Excel or text format on the MTS production server for SSN to EDIPI reconciliation. Upon receipt of the reconciled list from VA, the Contractor shall update the database primary identifier to EDIPI and set the SSN to secondary status in the legacy database if possible. The Contractor shall provide a Delta Patient List of names and SSNs added between the initial extract and go-live for subsequent identifier conversion. VHA will provide a reconciled list, and the Contractor shall perform the delta patient identifier change.

The Contractor shall collaborate with VA Healthcare Technology Management (HTM) staff to test EDIPI functionality as the primary identifier, identify and resolve any issues. Additionally, the Contractor shall collaborate work with VA to develop and adhere to a conversion schedule within the period of performance.

Deliverables:
A. Master List of Legacy Patient Records
B. Delta Patient List

5.13.2 VHA ELECTRONIC HEALTH RECORD (EHR) INTEGRATION

The Contractor shall provide an MTRS solution with separate and distinct production and test environments. The solution shall include an interface engine capable of managing HL7 messages to both VistA/CPRS and the Federal Electronic Health Record (FEHR) [Oracle Health EHR] simultaneously.

The Contractor shall implement HL7 Orders (ORM) and HL7 Results (ORU) interfaces between VA MTRS and both VA's EMRs (VistA CPRS and Federal Electronic Health Record [Oracle Health EHR]). Based on the project schedule, the Contractor shall integrate MTS at facilities with either VistA CPRS or Federal Electronic Health Record (FEHR). This is dependent on the facility's EHR at the time of go live.

The MTRS solution shall support multiple concurrent ORU/ORM HL7 connection pathways, including one production FEHR instance and multiple legacy VistA CPRS/VistA Imaging instances. For VA Medical Centers still using VistA CPRS, each VistA CPRS instance is unique to the facility and has its own IP address.

The Contractor shall perform all required testing and go-live activities for FEHR integration, including:

1. VA Enterprise Risk Assessment (ERA) specific to the FEHR interface documentation
2. Connectivity and smoke testing
3. Installation and configuration of HL7 interfaces on both test and production systems
4. Participation in Interface Solution Testing (IST) sessions with VA and Oracle
5. Attendance at planning activities such as dry runs and table-top exercises
6. Execution of FEHR interface cutover to production outside normal business hours
7. End-user training for workflows specific to FEHR integration.

Contractor shall develop a VA Vendor Integration Document (VID) in coordination with VA and Oracle Health. The VID will document any deviations from “Standardized Radiology Imaging Integration Interface Control Document” for the MTRS system.

The Contractor shall develop and deliver a FEHR Integration and Validation Checklist.

Deliverable:

A. VA Vendor Integration Document (VID)
B. FEHR Integration and Validation Checklist

5.14 OPTION PERIODS

The Contractor must provide all software licensing and support services necessary to ensure uninterrupted, fully compliant operational MTRS enterprise solution during Option Periods 1 through 4. The contractor must:

A. Furnish and maintain all software licenses required for the MTRS application, associated databases, reporting tools, and any integrated components necessary for full operational capability during the option period.
B. Ensure all licenses remain active, valid, and compliant with vendor terms, federal acquisition regulations, and applicable security and privacy requirements for the duration of the option period.
C. Provide technical support, customer service, and system sustainment in accordance with the requirements in Sections 5.1 through 5.13 of this PWS.
D. Provide technical support for all MTRS patches, security updates, bug fixes, enhancements, and version upgrades necessary to maintain system stability, security, and compliance.
E. Ensure support services include timely troubleshooting, issue resolution, and user assistance at service levels that meet or exceed the performance requirements identified in Section 5.
F. Maintain documentation of all licenses, renewals, updates, and support activities, and provide such documentation to the Government upon request.
G. Ensure that all licensing and support activities conducted during the option periods preserve full functionality, interoperability, and performance of the MTRS enterprise solution consistent with base year requirements.

All licensing and support services provided under this optional task shall comply with the same performance standards in Sections 5.1 through 5.13 of this PWS, deliverable requirements, security protocols, and quality measures applicable to the base period requirements in Sections 5.1 through 5.13 of this PWS,

5.15 OPTIONAL TASKS

This requirement includes up to six (6) optional tasks that the Government may exercise at any time during the performance period in accordance with the terms and conditions of the contract. The Contractor shall deliver and maintain an enterprise MTRS solution to meet all functional, technical, security, integration, and performance requirements identified in Sections 5.1 through Sections 5.13 of this PWS, when an optional task is exercised.

All work performed under an exercised optional task shall comply with the same standards, deliverables, acceptance criteria, and performance requirements applicable to the base effort.

5.15.1 OPTIONAL TASK 1: MTRS INCLUSIVE OF IMPLEMENTATION AND INTERFACE SERVICES

The contractor shall provide implementation and interfacing services for VHA Mammography programs, not to exceed quantity of 78 sites that will continue to meet all functional, technical, integration, security, and functionality requirements identified in section 5.1 through sections 5.13 of this PWS.

The Contractor shall provide a Post Go-Live Checklist for each site within five (5) business days following each site's go-live date. The Post Go-Live Checklist shall document all implementation milestones and tasks completed during the transition to operational status and shall reflect the finalized configuration, validation, and acceptance activities required to achieve full operational readiness.

The Contractor shall submit the completed checklist to the Government for review and confirmation within five (5) business days after the site's go-live date, or as otherwise specified in the delivery schedule.

Deliverables:

A. Post Go-Live Checklist

5.15.2 OPTIONAL TASK 2: DATA MIGRATION

The Contractor's fully functional MTRS solution shall include Data Migration and Data Migration Reports formatting of studies from the current Mammography information systems for all prior studies in advance of each respective VAMC go-live. The data migration shall not exceed the quantity of 20 sites. The data migration must include, at a minimum, the last five (5) years of data.

Prior to contract completion or termination, the Contractor shall deliver all MTS data in a user-accessible format, assume full responsibility for project management and associated costs. Furthermore, the Contractor shall provide the Department of Veterans Affairs with all administrative system and database credentials required for system management and sustainment.

The Contractor shall conduct data migration services and provide a data migration report for all VHA sites/legacy MTRS systems as listed in Addendum C. The data migration report must include a comprehensive list of all administrative MTRS system and database credentials available at the time of go-live.

Deliverable:
Data Migration Report

5.15.3 OPTIONAL TASK 3: AD HOC TRAINING SESSION - REMOTE

The Contractor's fully functional MTRS solution shall include remote clinical, system administrator, and Healthcare Technology Management (HTM) training as specified below. The ad hoc remote training session shall not exceed the quantity of 20 training weeks.

The Contractor shall provide Training Plan and Training Attendance Records for all personnel who participate in required training activities. All training documentation shall be delivered to the Government in a format acceptable within 5 business days after training completion.

Deliverables:
A. Training Plan
B. Training Attendance Records

5.15.4 OPTIONAL TASK 4: AD HOC TRAINING SESSION - IN PERSON

The Contractor's fully functional MTRS solution shall include in person clinical, system administrator, and Healthcare Technology Management (HTM) training as specified below. The ad hoc in person training session shall not exceed the quantity of 20 training weeks.

The Contractor shall provide Training Plan and Training Attendance Records for all personnel who participate in required training activities. All training documentation shall be delivered to the Government in a format acceptable within 5 business days after training completion.

Deliverables:
A. Training Plan
B. Training Attendance Records

5.15.5 OPTIONAL TASK 5: EHRM GO LIVE SUPPORT

The Contractor shall provide an MTRS solution with separate and distinct production and test environments. The solution shall include an interface engine capable of managing HL7 messages to both VistA/CPRS and the Federal Electronic Health Record (FEHR) [Oracle Health EHR] simultaneously. The EHRM go live support shall not exceed the quantity of 20 sites.

The Contractor shall implement HL7 Orders (ORM) and HL7 Results (ORU) interfaces between VA MTS and both VA's EMRs (VistA CPRS and Federal Electronic Health Record [Oracle Health EHR]). Based on the project schedule, the Contractor shall integrate MTS at facilities with either VistA CPRS or Federal Electronic Health Record (FEHR). This is dependent on the facility's EHR at the time of go live.

The MTS solution shall support multiple concurrent ORU/ORM HL7 connection pathways, including one production FEHR instance and multiple legacy VistA CPRS/VistA Imaging instances. For VA Medical Centers still using VistA CPRS, each VistA CPRS instance is unique to the facility and has its own IP address.

The Contractor shall perform all required testing and go-live activities for FEHR integration, including:

1. VA Enterprise Risk Assessment (ERA) specific to the FEHR interface documentation
2. Connectivity and smoke testing
3. Installation and configuration of HL7 interfaces on both test and production systems
4. Participation in Interface Solution Testing (IST) sessions with VA and Oracle
5. Attendance at planning activities such as dry runs and table-top exercises
6. Execution of FEHR interface cutover to production outside normal business hours
7. End-user training for workflows specific to FEHR integration.

Contractor shall develop a VA Vendor Integration Document (VID) in coordination with VA and Oracle Health. The VID will document any deviations from “Standardized Radiology Imaging Integration Interface Control Document” for the MTRS system.

The Contractor shall develop and deliver a FEHR integration and validation checklist.

The Contractor shall provide support services for a one-time patient identifier conversion and merge process within the legacy Mammography Tracking System (MTS) database. This effort shall include move/downgrade primary Medical Record Number (MRN) (Patient Identifier) that is currently Social Security Number (SSN) to a secondary Patient Identifier if possible and insert corresponding Electronic Data Interchange Personal Identifier (EDIPI) (New Patient Identifier) into the primary MRN field or status.

The Contractor shall compile and deliver a Master List of Legacy Patient Records, including SSNs and available attributes (e.g., Last Name, First Name, Date of Birth, Sex), in Excel or text format on the MTS production server for SSN to EDIPI reconciliation. Upon receipt of the reconciled list from VA, the Contractor shall update the database primary identifier to EDIPI and set the SSN to secondary status in the legacy database if possible. The Contractor shall provide a Delta Patient List of names and SSNs added between the initial extract and go-live for subsequent identifier conversion. VHA will provide a reconciled list, and the Contractor shall perform the delta patient identifier change.

The Contractor shall collaborate with VA Healthcare Technology Management (HTM) staff to test EDIPI functionality as the primary identifier, identify and resolve any issues. Additionally, the Contractor shall collaborate work with VA to develop and adhere to a conversion schedule within the period of performance.

Deliverables:

A. FEHR Integration and Validation Checklist
B. Master List of Legacy Patient Records
C. Delta Patient List

5.15.6 OPTIONAL TASK 6: AI CALCULATION TOOL (ENTERPRISE LICENSE)

The Contractor shall design, develop, validate, and deliver an AI-enabled risk calculation tool capable of generating individualized 5-year risk predictions based on

predefined clinical, demographic, or operational data inputs. The tool shall be offered and implemented as an enterprise license and meet the following requirements:

1. The Contractor shall develop or integrate an AI model development package capable of producing a 5year risk score with documented methodology. The Contractor shall ensure the model includes explainability features to support decision-making and operational transparency. The package should be streamlined for us within the overarching enterprise MTRS solution.
2. The contractor shall deliver an AI model requirements document (MRD) detailing description of data elements, model approaching, algorithms, and baseline assumptions.
3. The Contractor shall deliver a Validation and Test Report consisting of internal validation (e.g., cross-validation), internal validation results (accuracy, calibration, ROC, etc.), external validation results, and analyses of bias, fairness, and performance by subgroup. The Contractor must provide calibration metrics to demonstrate model accuracy and reliability. The Contractor shall conduct external validation using an independent dataset provided either by the Government or by the Contractor with Government approval.
4. The Contractor shall deliver a Technical Documentation Package detailing the model's data sources, assumptions, limitations, and governance controls. The Contractor shall identify and mitigate any model bias and provide testing results demonstrating equitable performance across demographic groups.
5. The Contractor shall deliver an Interface (API, dashboard, or module) that allows Government users to access the 5-year risk output within with the enterprise MTRS software. The Contractor shall ensure compatibility with Government systems as specified in the Task Order.
6. The Contractor shall deliver a Training Package including user training materials and conduct knowledge transfer sessions for Government personnel.
7. The Contractor shall deliver a Maintenance and Monitoring Plan for ongoing model retraining, recalibration, and performance reporting at intervals specified by the Government.

Deliverables:

A. AI Model Requirements Document (MRD)
B. AI Model Development Package
C. Validation and Test Report
D. Technical Documentation Package
E. AI Calculation Tool Interface
F. Training Package
G. Maintenance and Monitoring Plan

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

6.1.1 VA TECHNICAL REFERENCE MODEL

The Contractor shall comply with the VA OIT Technical Reference Model (VA TRM). Compliance with the VA TRM is achieved by using only technologies and standards that are listed as approved for use in the VA TRM. The Contractor shall provide all necessary information requested by VA to ensure TRM approval is obtained prior to use on VA's network.

6.1.2 ZERO TRUST – VA CRITICAL SECURITY CONTROLS

VA has established minimum mandatory security requirements and requires that any network connected software system or service must meet the VA Critical Security Controls as outlined in the VA Memorandum, "VA Security Controls", https://www.voa.va.gov/DocumentView.aspx?DocumentID=5010. VA Critical Security Controls identify the minimum mandatory requirements that must be implemented across all VA enterprise infrastructure, cloud computing environments, information systems, networks, and specialized devices (medical devices/systems, special-purpose systems, and research scientific computing devices) that process, store, and/or transmit VA data. Effective July 1, 2025, the Contractor shall implement these VA Critical Security Controls, within any network connected software system or service prior to being authorized for use in the VA. This functional requirement is not negotiable, and Plan of Action & Milestones (POAM) will not be accepted in the event these controls cannot be implemented for new systems. Critical Security Controls are intended to increase VA's security posture and provide security and privacy risk visibility into the VA network and is not a new requirement. The Contractor's failure to maintain these VA Critical Controls after implementation will result in VA discontinuing the use of the system.

6.1.3 FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM)

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are Personal Identity Verification (PIV) card-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Architecture (EA), and VA Identity and Access Management (IAM) approved Enterprise Technology Guidelines (ETG). The Contractor shall ensure all Contractor delivered applications and systems comply with the VA Identity, Credential, and Access Management policies and guidelines set forth in Executive Order 14028, VA Handbook 6510 VA Identity and Access Management, VA Handbook 0735 Homeland Security Presidential Directive 12 (HSPD-12) Program, CISA Binding Operational Directive 23-01, and align with the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance v2.0.

The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-4, VA Handbook 6500, and VA IAM enterprise requirements for direct, assertion-based authentication, and/or trust based

authentication, as determined by the ETGs. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of PIV card and/or Common Access Card (CAC), as determined by the business need.

The Contractor shall ensure all Contractor delivered applications and systems conform to the specific Identity and Access Management PIV requirements set forth in the Office of Management and Budget (OMB) Memoranda M-05-24, M-19-17, M-22-09, and NIST Federal Information Processing Standard (FIPS) 201-3. Contractor delivered applications and systems shall be on the FIPS 201 Approved Product List (APL). If the Contractor delivered application and system is not on the APL, the Contractor shall be responsible for taking the application and system through the FIPS 201 Evaluation Program.

The Contractor shall ensure all Contractor delivered applications and systems support:

1. Automated provisioning and are able to use enterprise provisioning service.
2. Interfacing with VA's Master Person Index (MPI) to provision identity attributes, if the solution relies on VA user identities. MPI is the authoritative source for VA user identity data.
3. The VA defined unique identity (Secure Identifier [SEC ID] / Integrated Control Number [ICN]).
4. Multiple authenticators for a given identity and authenticators at every Authenticator Assurance Level (AAL) appropriate for the solution.
5. Identity proofing for each Identity Assurance Level (IAL) appropriate for the solution.
6. Federation for each Federation Assurance Level (FAL) is appropriate for the solution, if applicable.
7. Two-factor authentication (2FA) through an applicable Technology Guideline as outlined in VA ETG.
8. A Security Assertion Markup Language (SAML) implementation if the solution relies on assertion-based authentication. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST SP 800-63-3 guidelines.
9. Authentication/account binding based on trusted Hypertext Transfer Protocol (HTTP) headers if the solution relies on Trust based authentication.
10. Role Based Access Control.
11. Auditing and reporting capabilities.
12. Compliance with VIEWS 00155984, PIV Logical Access Policy Clarification https://www.voa.va.gov/DocumentView.aspx?DocumentID=4896.

The required Assurance Levels for this specific effort are Identity Assurance Level 3, Authenticator Assurance Level 3, and Federation Assurance Level 3.

6.1.4 INTERNET PROTOCOL VERSION 6 (IPv6)

The Contractor solution shall support IPv6-Only based upon the memo issued by the Office of Management and Budget (OMB) on November 19, 2020 (https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf). Which defines IPv6-only as the state of an operational system or service when IPv4 protocol functions (addressing, packet forwarding) are not in use. The NIST USGv6 profile defines technical requirements for a product to be capable of operating in IPv6-Only environments. IPv6-Only technology, in accordance with the USGv6 Program (https://www.nist.gov/programs-projects/usgv6-program/usgv6-revision-1), NIST Special Publication (SP) 500-267B Revision 1 "USGv6 Profile" (https://doi.org/10.6028/NIST.SP.500-267Br1), and NIST SP 800-119 "Guidelines for the Secure Deployment of IPv6" (https://doi.org/10.6028/NIST.SP.800-119), compliance shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. In addition to the above requirements, all devices, applications, and systems shall support all applicable functionality on native IPv6-Only as well as dual stack (IPv6 / IPv4) connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g., web, email, DNS, ISP services, etc.) shall support native IPv6-Only and dual stack (IPv6 / IPv4) users and all internal infrastructure and applications shall support using native IPv6-Only and dual stack (IPv6 / IPv4) for all functionality and operations.

6.1.5 TRUSTED INTERNET CONNECTION (TIC)

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M-19-26, "Update to the Trusted Internet Connections (TIC) Initiative" (https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf), VA Directive 6513 "Secure External Connections", and shall comply with the TIC 3.0 Core Guidance Documents, including all Volumes and TIC Use Cases, found at the Cybersecurity & Infrastructure Security Agency (CISA) (https://www.cisa.gov/publication/tic-30-core-guidance-documents).

6.1.6 STANDARD COMPUTER CONFIGURATION

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, Windows 11, Edge (Chromium based), and 365 Apps for enterprise. Applications delivered to VA and intended to be deployed to Windows 11 workstations shall be delivered as a signed .msi package with switches for silent and unattended installation and updates shall be delivered in signed .msp file formats for easy deployment using Microsoft Endpoint Configuration Manager (CM) VA's current desktop application deployment tool. Signing of the software code shall be through a vendor provided certificate that is trusted by VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the Defense Information Systems Agency (DISA) Secure Technical Implementation Guide (STIG) specific to the particular client operating system being used.

6.1.7 VETERAN FOCUSED INTEGRATION PROCESS (VIP) AND PRODUCT LINE MANAGEMENT (PLM)

The Contractor shall support VA efforts IAW the Veteran-Focused Integration Process (VIP) Guide and Product Line Management (PLM) Playbook. The major focus of VIP is on Enterprise Oversight, Governance, reporting, and establishing practices that focus on outcomes and continuously delivering sustainable IT capabilities to benefit the Veteran. PLM is a framework that focuses on delivering functional products that provide the highest priority work to customers while delivering simplified, reliable, and practical solutions to the business, medical staff, and our Veterans. The VIP Guide is a companion guide to the PLM Transformation Playbook and can be found at: https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371 and the PLM Transformation Playbook can be found at https://www.voa.va.gov/DocumentView.aspx?DocumentID=4946. VIP and PLM are the authoritative processes that IT projects must follow to ensure development and delivery of IT products.

The VIP Guide provides guidance for transitioning from project-centric to product-centric delivery. The VIP guide applies to all OIT Office of Management and Budget (OMB) reportable products that are required to collect and report costs, schedules, risks, and other valuable information in VA PARS (whether products are procured or developed by VA) and any VA Information Technology project effort in Software Product Management (SPM) and Infrastructure Operations (IO), or their successors, that touch the VA network regardless of IT organizational alignment (whether it spends government funding from VA's Congressional IT Appropriation or any other appropriation).

The PLM Transformation Playbook details how OIT leadership expects Product Lines (PLs) to implement PLM, DevOps, and Lean-Agile principles, methods, practices, and techniques through levels of maturity. The PLM Transformation Playbook applies to all Information Technology (IT) products aligned to PLs in the Software Product Management, Infrastructure Operations and Product Engineering organizations within the OIT organization.

Others outside the referenced groups or organizations may use the VIP Guide and PLM Transformation Playbook for situational awareness as needed.

6.1.8 PROCESS ASSET LIBRARY (PAL)

The Contractor shall perform their duties consistent with the processes defined in the OIT Process Asset Library (PAL). The PAL includes a spectrum of OIT functions and activities, such as project management, operations, service delivery, communications, acquisition, and resource management. PAL serves as an authoritative and informative repository of searchable processes, activities or tasks, roles, artifacts, tools and applicable standards and guides to assist the OIT workforce, Government and Contractor personnel. OIT utilizes PAL processes to ensure compliance with policies and regulations and to meet VA quality standards. The PAL includes the contractor onboarding process consistent with Section 6.2.2 and can be found at

process_CONB_ext.docx (live.com). The main PAL can be accessed at www.va.gov/process.

6.1.9 AUTHORITATIVE DATA SOURCES

The VA Enterprise Architecture Repository (VEAR) is one component within the overall EA that establishes the common framework for data taxonomy for describing the data architecture used to develop, operate, and maintain enterprise applications. The Contractor shall comply with the department's Authoritative Data Source (ADS) requirement that VA systems, services, and processes throughout the enterprise shall access VA data solely through official VA ADSs where applicable, see below. The Information Classes which compose each ADS are located in the VEAR, in the Data & Information domain. The Contractor shall ensure that all delivered applications and system solutions support:

1. Interfacing with VA's Master Person Index (MPI) (formerly the Master Veteran Index (MVI)) to provision identity attributes, if the solution relies on VA user identities. MPI is the authoritative source for VA user identity data.
2. Interfacing with Capital Asset Inventory (CAI) to conduct real property record management actions, if the solution relies on real property records data. CAI is the authoritative source for VA real property record management data.
3. Interfacing with electronic Contract Management System (eCMS) for access to contract, contract line item, purchase requisition, offering vendor, and solicitation information above the micro-purchase threshold, if the solution relies on procurement data. ECMS is the authoritative source for VA procurement actions data.
4. Interfacing with HRSmart Human Resources Information System to conduct personnel action processing, on-boarding, benefits management, and compensation management, if the solution relies on personnel data. HRSmart is the authoritative source for VA personnel information data.
5. Interfacing with VA Profile to access personal contact information, if the solution relies on VA Veteran personal contact information data. VA Profile is the authoritative source for VA Veteran Personal Contact Data.
6. Interfacing with VA/Department of Defense (DoD) Identity Repository (VADIR) for determining eligibility for VA benefits under Title 38, if the solution relies on qualifying active-duty military service data. VADIR is the authoritative source for qualifying active-duty military service in VA.
7. Interfacing with VA Systems Inventory (VASI) to access VA systems information, if the solution relies on VA system information. VASI is the authoritative source for VA Information Technology systems.
8. Interfacing with Enterprise Mission Assurance Support Service (eMASS) to access the historical Authority to Operate (ATO) status of all VA Information Systems prior to migrating to ServiceNow Continuous Authorization and Monitoring (SNowCAM) until it is determined the migration is completed and eMASS is sunset. eMASS contains the historical Authority to Operate (ATO) status of all VA Information Systems prior to September 30, 2025, with all status provided through SNowCAM once migration is completed.

6.1.10 SOCIAL SECURITY NUMBER (SSN) REDUCTION

The Contractor solution shall support the Social Security Number (SSN) Fraud Prevention Act (FPA) of 2017 which prohibits the inclusion of SSNs on any document sent by mail. The Contractor support shall also be performed in accordance with Section 240 of the Consolidated Appropriations Act (CAA) 2018, enacted March 23, 2018, which mandates VA to discontinue using SSNs to identify individuals in all VA information systems as the Primary Identifier. The Contractor shall ensure that any new IT solution discontinues the use of SSN as the Primary Identifier to replace the SSN with the ICN in all VA information systems for all individuals. The Contractor shall ensure that all Contractor delivered applications and systems integrate with the VA MPI for identity traits to include the use of the ICN as the Primary Identifier. The Contractor solution may only use a Social Security Number to identify an individual in an information system if and only if the use of such number is required to obtain information VA requires from an information system that is not under the jurisdiction of VA.

6.1.11 SOFTWARE AND LICENSING REQUIREMENTS

The Contractor shall be responsible for the provision of all software licenses and any associated licensing maintenance required for any development, delivery, integration, operation, and/or maintenance associated with its proposed application(s), software products, software solution, and/or system including, but not limited to, any and all application(s), software and/or software products that comprise, are a part of, or integrate with the Contractor’s proposed application(s), software products, software solution, and/or system for the life of any resulting contract.

6.1.12 GENERATIVE ARTIFICIAL INTELLIGENCE REQUIREMENTS

If Artificial Intelligence (AI) is part of the Contractor system/solution, the Contractor shall be in compliance with E.O. 13960 and 14319, OMB Memorandums M-25-21, M-25-22, and M-26-04, and VA Directive and Handbook 6500 to support VA in trustworthy, secure, responsible, accountable, Truth Seeking, and Ideologically Neutral AI innovation.

The Contractor shall protect VA Sensitive data from unauthorized disclosure or use, and from being used to train or improve the functionality of the vendor's commercial offerings without express permission from VA. Only VA-hosted instances of generative AI services may be approved for use with VA-sensitive data. Current guidance and approved AI tools are available here: https://department.va.gov/ai/guidance-for-generative-ai-use-at-va/. The entire definition of VA Sensitive Data can be found at 38 U.S.C. § 5727 (23).

The Contractor shall deliver the services, technical data, configurations, models, weights, documentation or other information, including source code, developed during contract performance. The Contractor, in collaboration with VA, must evaluate the output of any AI tool for accuracy prior to using the output in VA efforts. All data, including models, weights, algorithms, and outputs generated using either Government-furnished data or data first developed under this contract shall be the property of the

Government with unlimited rights as defined by FAR 52.227-14. The Contractor shall also deliver any custom-developed code developed with AI methodologies in accordance with the SHARE IT Act, if applicable. VA shall also retain unlimited rights to any improvements to that data, including the continued design, development, testing, and operation of AI systems and/or systems utilizing AI.

The Contractor shall ensure that all AI Systems, including Large Language Models (LLM), whether standalone LLMs or integrated into broader software platforms, procured under this effort and/or used in performance of this contract complies with the Unbiased AI Principles as defined in Executive Order 14319 and OMB Memorandum M-26-04, e.g. Truth Seeking and Ideologically Neutral, as applicable to the intended use of the system.

The Contractor shall ensure that AI System/LLM generated outputs are truthful in responding to user prompts seeking factual information or analysis, prioritize historical accuracy, scientific inquiry, and objectivity, as well as acknowledge uncertainty where reliable information is incomplete or contradictory and do not fabricate, hallucinate, or present unverifiable information as fact.

The Contractor shall ensure that LLMs and AI outputs are neutral, nonpartisan tools that do not manipulate responses in favor of ideological dogmas such as Diversity, Equity, and Inclusion (DEI). The Contractor shall ensure that the LLMs, including the AI System, are not intentionally encoded with partisan or ideological judgments within an AI System's/LLM's outputs unless those judgments are prompted by or otherwise readily accessible to the end user.

Compliance with the AI requirements of this contract, including adherence to the Unbiased AI Principles, Truth-Seeking and Ideological Neutrality requirements, disclosure obligations, monitoring and reporting requirements, and corrective action responsibilities, is a material condition of eligibility for payment and continued performance. In accordance with OMB Memorandum M-26-04, failure to comply with these requirements, or refusal to take timely and appropriate corrective action to remedy identified noncompliance, may constitute a material breach of contract and may result in remedies consistent with the terms of the contract and applicable law including but not limited to withholding of payment, termination for cause/default, or other appropriate contractual remedies, as determined by the Contracting Officer.

All AI for delivery and/or use in performance of the contract shall adhere to the *VA Trustworthy AI Framework*, available at https://department.va.gov/ai/trustworthy/. Once the Contractor has obtained CO authorization to use specific AI in contract performance, the Contractor shall provide the COR a signed Statement of Attestation prior to AI implementation as identified in the Artificial Intelligence in VA Contracts clause, to include its associated list of AI being used in contract performance.

Deliverable:
Statement of Attestation

6.1.12.1 AI SYSTEM/LLM DEVELOPMENT AND OPERATION DOCUMENTATION REQUIREMENTS

To enable Government continued assessment of compliance with Trustworthy AI requirements and both Unbiased AI Principles, Truth-seeking and Ideological Neutrality, in accordance with OMB M-26-04, the Contractor shall provide AI System/LLM Development and Operation Documentation Package to include, at a minimum:

1. **Acceptable Use Policy**

The Contractor shall provide an Acceptable Use Policy document governing its AI operation that characterizes and differentiates appropriate and inappropriate use of their product offering.

2. **Model Cards, System Cards and/or Data Cards**

The Contractor shall provide documentation describing essential information about the model, system, and or data as it relates to the AI/LLM product offering. The documentation shall address summaries of training process, identified risks and mitigations, and model evaluation scores on LLM benchmarks at a minimum, where appropriate.

3. **End User Resources**

The Contractor shall provide documentation to include product tutorials, developer guides, and/or other tools to assist VA in ensuring proper use of the AI/LLM to maximize utility.

4. **Mechanism for End User Feedback**

The Contractor shall provide documentation describing the mechanism employed to provide feedback to the Offeror on outputs identified that violate the Unbiased AI Principles. This may be satisfied by a general inbox, specific Point of Contact, or similar feedback mechanism.

5. **Pre-Training and Post-Training Activities of the AI System/LLM**

The Contractor shall provide documentation of Pre-Training and Post Training Activity that provides details on:

a. Actions taken that impact the factuality and grounding of AI System/LLM outputs
b. System-level prompts that provide natural language instructions to the model specifying guidelines on responding to user-generated queries, to include how a model responds when reliable information is incomplete, contradictory, or subject to individual interpretation
c. The type of outputs restricted via content moderation and safety filters
d. The use of red teaming as a means of continuously assessing the model to protect against incidents of bias in generated output.

e. Training or development, if any, that occurred outside the United States, to include the type of activity and the country in which it occurred.
f. Any modifications or configurations undertaken to comply with any regulation from a government other than the U.S. Federal Government.

6. **Model Evaluation Results and Methodologies**

The Contractor shall provide documentation describing the Evaluation Results of bias evaluations conducted by the Vendor to include the methodology for performing such tests (e.g., testing prompt pairs for politically oriented topics).
The documentation shall also include Benchmark scoring results measuring the model's bias, helpfulness, honesty, or accuracy when provided with ambiguous versus straightforward questions. (Including any benchmarks comparing performance across multiple languages, where applicable).

7. **Description of Enterprise-Level Controls**

The Contractor shall provide documentation describing the Enterprise Governance tools and controls, such as:

a. Customizable system instructions that are additive to a base model's system prompts or content generation filters.
b. Product features that require a model to cite sources of its outputs or otherwise provide visibility into the provenance of the model's outputs.
c. AI System/LLM model evaluation tools that enable comparisons either between a model's outputs, or across various models.

8. **Third Party Modification Disclosure**

The Contractor shall disclose any additional controls to modify an AI Model's/LLM's output applied by the Contractor if the Contractor is not a direct developer of the LLM (e.g., classifiers, system prompts, fine-tuning, content moderation and filters, etc.)

Deliverable:
A. AI System/LLM Development and Operation Documentation Package

6.1.12.2 MONITORING, REPORTING, AND CORRECTIVE ACTION

The Contractor shall develop and implement a Compliance Monitoring and Reporting Plan supporting ongoing monitoring processes to evaluate AI outputs for compliance with Trustworthy AI and Unbiased AI principles. This plan shall include the mechanism for authorized users to provide end user feedback to report suspected violations of Truth-Seeking or Ideological Neutrality requirements.

The Contractor shall notify the COR within 10 business days of identifying any material deviation from these principles and shall submit a written Corrective Action Plan describing mitigation steps, responsible parties, and timelines. Any material deviation, corrective action taken, and results shall be detailed in the Monthly Progress Reports.

Deliverables:
A. Compliance Monitoring and Reporting Plan
B. Corrective Action Plan

6.1.12.3 AI MODEL UPDATES AND CHANGE DISCLOSURES

The Contractor, in an AI Model/LLM Change Disclosure, shall notify the Government throughout the PoP in advance of any material changes to AI models, including new AI enhancements, features and/or components, controls, retraining, classifiers, system prompts, fine-tuning, content moderation, filters, version replacement, or architectural changes, that could reasonably affect compliance with Trustworthy AI or Unbiased AI principles. Updated documentation shall be provided to VA for VA approval prior to implementation of such changes.

Deliverable:
A. AI Model/LLM Change Disclosure

6.1.13 SOURCE CODE HARMONIZATION AND REUSE IN INFORMATION TECHNOLOGY (SHARE IT Act)

The Contractor shall comply with the Source Code Harmonization and Reuse in Information Technology (SHARE IT) Act, P.L. 118-187, when developing and delivering custom code first produced for the VA in the performance of this Contract/Order. The Contractor shall deliver to the Government all data first produced under this Contract/Order with unlimited rights as defined by FAR 52.227-14, to include without limitation, all custom-developed code and other key technical components of the code (including documentation, data models, schemas, metadata, architecture designs, configuration scripts, and artifacts required to develop, build, test, and deploy the code). Custom-developed code includes source code, or segregable portions of source code and all documentation created in support thereof to include source code written for a software project, product, module, plugin, script, middleware, or application programming interface.

6.2 SECURITY AND PRIVACY REQUIREMENTS

It has been determined that protected health information may be disclosed or accessed, and a signed Business Associate Agreement (BAA) shall be required. The Contractor shall adhere to the requirements set forth within the BAA, referenced in Section D of the contract, and shall comply with VA Directive 6066.

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

In accordance with VA Handbook 0710, Personnel Vetting Program, the position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the PWS are:

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.1	☒	☐	☐
5.2	☒	☐	☐
5.*3*	☒	☐	☐
5.4	☒	☐	☐
5.5	☒	☐	☐
5.6	☒	☐	☐
5.7	☒	☐	☐
5.8	☒	☐	☐
5.9	☒	☐	☐
5.10	☒	☐	☐
5.11	☒	☐	☐
5.12	☒	☐	☐
5.13	☒	☐	☐
5.14	☒	☐	☐
5.15	☒	☐	☐

The Tasks identified above and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the particular Contractor individual will be working. The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each Contractor individual based upon the tasks the Contractor individual will be working, in accordance with their submitted proposal.

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak, and understand the English language.

b. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the PAL template artifact. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2.1 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall

remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 (or its successor) are to encrypt the file, use a secure fax, or use a traceable mail service. (Note that by September 22, 2026, all FIPS 140-2 certificate validations will be placed on the Historical List. See FIPS Transition Effort Timeline for more details: https://csrc.nist.gov/projects/fips-140-3-transition-effort#schedule)

c. The Contractor should coordinate with the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized. The Contractor shall bring their completed Personnel Security Adjudication Center (PSAC) Fingerprint request form with them (see paragraph d.4. below) when getting fingerprints taken.

d. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
    1) Optional Form 306
    2) Self-Certification of Continuous Service
    3) VA Form 0710
    4) Completed PSAC Fingerprint Request Form

e. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Defense Counterintelligence and Security Agency (DCSA) National Background Investigation Services (NBIS) Electronic Application (eAPP) (formerly e-QIP) after receiving an email notification from the PSAC.

f. The Contractor employee shall certify and release the eAPP document, print, and sign the signature pages, and send them encrypted to the COR for electronic submission to the PSAC. These documents shall be submitted to the COR within 3 business days of receipt of the eAPP notification email. (Note: DCSA is moving towards a “click to sign” process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via eAPP).

g. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.

h. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC), completed training delineated in VA Handbook 6500.6 (Appendix C, Section 4), signed “Contractor Rules of Behavior”, and with a valid, operational Personal Identity Verification

(PIV) credential for PIV-only logical access to VA's network. A PIV card credential can be issued once your SAC has been favorably adjudicated and your background investigation has been scheduled by DCSA. However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of DCSA.

i. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.

j. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.

k. PIV Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

Deliverable:
Contractor Staff Roster

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include Microsoft 365 suite, MS Word, MS Excel, MS PowerPoint, MS Project, MS Access, MS Visio, AutoCAD, and Adobe Postscript Data Format (PDF).

6.4 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Levels of Performance associated with this effort.

PWS Section/ Deliverable	Measurement/Metric	Deliverable Timeline	Method of Surveillance	Surveillance Frequency	Acceptable Quality Level (AQL)
PWS 5.0 Fully Functioning MTRS	30 VA Mammography Program sites have gone live and are fully functional with respect to data migration, HL7 interface validation, PowerScribe integration, and clinical workflow reporting requirements within the base period.	12 months from the date of award.	Inspection by the COR, Project implementation tracking tool	Monthly	All 30 of base year VAMC sites have gone live with the MTRS solution within 12 months of contract award.
PWS 5.1.1 Contractor Project management plan	A completed project management plan that lays out the contractor's approach, work breakdown structure (WBS), timeline, and tools to be used in execution of the contract.	Completed and sent to VA three (3) weeks after contract award.	Review of deliverable by COR and VHA project management team.	VHA review within three weeks after receipt, and review monthly there on out.	A fully completed project planned received within 3 weeks after contract award.
PWS 5.1.2 Monthly progress reports	Monthly report covering all work completed during the reporting period and work planned for the subsequent month. Any problems should be highlighted with plan to resolve.	Within one (1) week after the end of the reporting period (month)	Inspection by the COR and VHA project management team	Monthly	No more than two (2) late progress reports were received within the period of performance.
PWS 5.2.1 Breast Examination Capability Statement	Capability statement for MTRS solution that outlines supported reporting for breast examination types.	As part of RFP response and within three (3) weeks after contract award.	Inspection by the COR and VHA project management team	VHA to review as part of RFP evaluation and within three (3) weeks after contract award.	Capability statement received as part of RFP response and within 3 weeks after contract award.
PWS 5.2.3 System interface and integration workflow validation checklist	Validation checklist showing that all interfaces and system integration requirements as listed in PWS 5.2.3 are met.	Prior to go live milestones	Inspection by COR and VHA project management team	Monthly, and 3 weeks prior to go live milestones	100% of features and requirements must be implemented with the MTRS solution.

PWS Section/ Deliverable	Measurement/Metric	Deliverable Timeline	Method of Surveillance	Surveillance Frequency	Acceptable Quality Level (AQL)
PWS 5.2.4 Patient data collection screenshots.	Screenshot showing patient data collection and breast cancer risk assessment features.	As part of RFP response and within three (3) weeks after contract award.	Inspection by COR and VHA project management team	VHA to review as part of RFP evaluation and within three (3) weeks after contract award.	100% of features and requirements must be implemented with the MTRS solution.
PWS 5.2.4 Patient Data collection tablets 6550 document.	Completion of 6550 by contractor for any proposed intake tablet offerings	As part of RFP response and reviewed within one (1) month from contract award	Inspection by COR and VHA project management team	VHA to review as part of RFP evaluation and within 3 weeks after contract award.	Completion of all applicable fields in the 6550 as reviewed by HTM.
PWS 5.2.5 Functional User Communication Process	Provide a functional user communication process that enables Radiologists and Technologists to enter or delete comments within the system and annotate the patient history form with clinical findings	Assessed prior to each VAMC go-live	Inspection by COR and VHA project management team	Due within 3 weeks of each VAMC Go-Live	Functional user communication process review prior to each go live.
PWS 5.2.6 Functional MTRS Radiologist Workflow	Validation that all user communication requirements as listed in PWS 5.2.6 are met.	prior to go live milestones	Inspection by COR and VHA project management team	Due within 3 weeks of each VAMC Go-Live	100% of features and requirements must be implemented with the MTRS solution.
PWS 5.2.7 Patient Tracking Screenshots	Demonstrate functionality through screenshots for requirements as listed in PWS 5.2.7.	As part of the RFP response and 3 weeks prior to go live milestones.	Inspection by COR and VHA project management team	Due within 3 weeks of each VAMC Go-Live	100% of features and requirements must be implemented with the MTRS solution as demonstrated through the screenshots.
PWS 5.2.8 Functional MTRS patient lay summary letters workflow	MTRS workflow that seamlessly sends the patient lay summary letters to VISTA/CPRS & FEHR in association with the final report or images.	Assessed prior to each VAMC go-live	Inspection by COR and VHA project management team	Due within 3 weeks of each VAMC Go-Live	100% of features and requirements must be implemented with the patient lay summary letter workflow.

PWS Section/ Deliverable	Measurement/Metric	Deliverable Timeline	Method of Surveillance	Surveillance Frequency	Acceptable Quality Level (AQL)
PWS 5.2.9 Compliance, Analytics, and Reporting screenshots.	The Contractor shall provide compliance, data analytics, and reporting screenshots illustrating the system's functionalities in reference to requirements as listed in PWS 5.2.9.	As part of RFP response, and prior to each go live.	Inspection by COR and VHA project management team	Due within 3 weeks of each VAMC Go-Live	100% of features and requirements must be implemented with the MTRS solution.
PWS 5.2.9.1 AI risk score calculation tool capability statement	The Contractor shall describe existing or future capabilities for the MTRS solution to integrate a 5-year risk score AI tool.	As part of RFP response, and 1 month after award.	Inspection by COR and VHA project management team	As part of RFP response, and 1 month after award.	Capability statement must show current offerings of any AI risk score features.
PWS 5.3 Hardware specifications and network requirements, including completion of VA Form 6550 and MDS2 document.	Receipt of all hardware specs, networking requirements, MDS2 document, and VA Form 6550	Within one month of contract award	Inspection by COR and VHA project management team	Within one month of contract award, and weekly thereafter if modifications /updates are required.	100% of technical documents must be provided
PWS 5.3 Disaster Recovery Plan	Comprehensive disaster recovery plan including internal backup processes/ functionality/tools, restoration, and summary of 3rd party backup agents allowed.	3 weeks Prior to first site go live.	Inspection by COR and VHA project management team	3 weeks prior to first VAMC go live and reviewed quarterly.	Comprehensive disaster recovery plan documentation received and reviewed by first site go live.
PWS 5.3 Production and Testing System Architecture	The contractor shall provide a system architecture that incorporates production and test system environments/servers for system change management testing.	Due at least 2 months Prior to first site go live.	Inspection by COR and VHA project management team	2 months prior to first go live site and assessed after change management events using the test environment	Production and test environment review and full functionality prior to first site go live.
PWS 5.3 MTRS Cloud Deployment Capability Report	MTRS cloud deployment capability report summarizing FEDRAMP status for cloud deployment, and whether the proposed MTRS solution can be implemented in the VA Enterprise Cloud Environment (VAEC)	Include in RFP response and within 3 weeks of contract award	Inspection by COR and VHA project management team	Include in RFP response and within 3 weeks of contract award	Cloud deployment capability report with capability summaries for both VAEC and FEDRAMP.

PWS Section/ Deliverable	Measurement/Metric	Deliverable Timeline	Method of Surveillance	Surveillance Frequency	Acceptable Quality Level (AQL)
PWS 5.3 Database Licensing	The contractor shall provide turnkey licensing for all databases (e.g. SQL, Oracle) required for the MTRS deployment.	Due after VA server deployment and review quarterly.	Inspection by COR and VHA project management team	Due after VA server deployment and review quarterly.	100% of database licenses required for enterprise MTRS solution shall be provided.
PWS 5.4 Enterprise Software Licenses	Enterprise MTRS software licensing with unlimited users across VHA.	Per VAMC go-live and reviewed annually	Inspection by COR and VHA project management team	Due 3 weeks prior to first site go live and reviewed Per VAMC go-live, and annually.	100% of VAMC user should be licensed (on an as needed basis)
PWS 5.6 Data Migration Report	Data migration report summarizing data sets migrated and reports formatting of studies from legacy information systems. The data migration must include, at a minimum, the last five (5) years of data for that respective site/VISN.	Prior to each VAMC go live	Inspection by COR and VHA project management team	Due 3 weeks Prior to each VAMC go live	100% of VAMC listed in PWS Addendum C Must have Data migration completed
PWS 5.6 MTRS data export in a user-accessible format	An export of all MTRS data in a user accessible format	Prior to the completion or termination of the contract	Inspection by COR and VHA project management team	Due 2 weeks Prior to the completion or termination of the contract	100% of MTRS data must be presented to VA in a user accessible format as deemed acceptable by the VA
PWS 5.6 MTRS administrative system and database credentials.	A list of all administrative MTRS system and database credentials needed to manage the enterprise servers.	3 weeks prior to the first VAMC go live and reviewed quarterly.	Inspection by COR and VHA project management team	3 weeks prior to the first VAMC go live and reviewed quarterly.	100% of admin account information required to manage the application and databases must be provided.
PWS 5.7 Quarterly Review Certification for System performance	Reviewing VHA data for system performance requirements outlined in 5.7.	Evaluation starts after first VAMC go live	Inspection by COR and VHA project management team	Reviewed quarterly after first VAMC go live	99% uptime for MTRS enterprise system. Downtime caused/initiated by VA factors does not count against the vendor.
PWS 5.8 User and Group Functionality Validation Report	Validation report that all user and group functionality requirements as listed in PWS 5.8 are met prior to each VAMC go live.	Prior to each VAMC go live	Inspection by COR and VHA project management team	Prior to each VAMC go live	100% of features and requirements must be implemented with the MTRS solution.

PWS Section/ Deliverable	Measurement/Metric	Deliverable Timeline	Method of Surveillance	Surveillance Frequency	Acceptable Quality Level (AQL)
PWS 5.9 Bi-directional HL7 Integration Validation Report	Validation report showing successful bi-directional HL7 integration to both VistA and FEHR as outlined in PWS 5.9. (each site will have one or the other)	Prior to each VAMC go live	Inspection by COR and VHA project management team	Prior to each VAMC go live	100% of VAMC in scope of the project must have validated HL7 integration with either Vista or FEHR.
PWS 5.10 DICOM conformance statements	DICOM conformance statements showing capability for standardized messaging	Within 1 month of contract award	Inspection by COR and VHA project management team	Within 1 month of contract award	Any DICOM products associated with the MTRS solution must be DICOM compliant.
PWS 5.11 Training Plan Training Attendance Records Training Quick Reference Guides	Training plan, attendance records, and quick reference guides for Clinical, system admin, and technical training as outlined PWS 5.11.	Prior to each VAMC go live	Inspection by COR and VHA project management team	3 weeks Prior to each VAMC go live	100% of VAMC in scope of the project must receive the required training.
PWS 5.11.4 Service Manuals	Clinical user and technical administrator service manuals for the system in an electronic format.	Prior to the first VAMC training date.	Inspection by COR and VHA project management team	3 weeks Prior to the first VAMC training date.	Inspection of the manuals received by the COR.
PWS 5.12 Customer Support Status Report	Customer support status report showing monthly tickets and turnaround times against requirements as outlined in PWS 5.12.	Evaluation starts after first VAMC go live	Inspection by COR and VHA project management team	Reviewed semi-annually after first VAMC go live	Customer support service within response times and target restoration times based on severity level outlined in PWS 5.12.
PWS 5.12 Software Obsolescence Plan	Software obsolescence, major upgrades, revisions, patches and fixes for the contract period.	Evaluation starts after first VAMC go live	Inspection by COR and VHA project management team	Reviewed semi-annually after first VAMC go live	Knowledge transfer, software upgrades support, and patching for all MTRS software changes as required VHA.

PWS Section/ Deliverable	Measurement/Metric	Deliverable Timeline	Method of Surveillance	Surveillance Frequency	Acceptable Quality Level (AQL)
PWS 5.13.1 EHRM Transition Support Services - SSN/EDIPI conversion	Master patient list and delta patient list to support transition from social security number to EDIPI.	Evaluation prior to each VAMC FEHR Go live. With master list due no more than 4 weeks before facility go live, and delta list within 5 days of the system cutover.	Inspection by COR and VHA project management team	2 months prior to VAMC FEHR go live and then weekly until cutover.	100% of VAMC in scope of the project that transition to FEHR must receive these services and support.
PWS 5.13.2 EHRM Transition Support Services - FEHR integration and validation checklist	FEHR integration and validation checklist per EHRM site transition outlining completed required testing activities.	Evaluation during each VAMC FEHR Go live	Inspection by COR and VHA project management team	Prior to each VAMC FEHR Go Live	100% of features and requirements must be implemented with the MTRS solution, as needed per EHRM transition.
PWS 5.14 Option Periods	Customer support and enterprise MTRS status report showing monthly tickets, turnaround times, and enterprise licensing customer complaints against requirements as outlined in PWS 5.12.	Evaluation starts after first option period is exercised.	Inspection by COR and VHA project management team	Reviewed semi-annually after first VAMC go live	Customer support service within response times and target restoration times based on severity level outlined in PWS 5.12. No more than five (5) customer complaints regarding enterprise licensing within the option period.
PWS 5.15.1 Optional Tasks: MTRS Implementation and Interface Services Post Go Live Checklist	Completion of post go-live checklist showing all completed implementation and integration milestones completed per site	Within 12 months of optional task being exercised, per site.	Inspection by COR and VHA project management team	Reviewed monthly upon optional task being exercised	100% of sites included in optional task must go live and have completed post go live checklist.

PWS Section/ Deliverable	Measurement/Metric	Deliverable Timeline	Method of Surveillance	Surveillance Frequency	Acceptable Quality Level (AQL)
PWS 5.15.2 Optional Task: Data Migration Report	Data migration report summarizing data sets migrated and reports formatting of studies from legacy information systems. The data migration must include, at a minimum, the last five (5) years of data for that respective site/VISN.	Prior to VAMC go live, or within 12 months of optional task if no go live involved.	Inspection by COR and VHA project management team	Reviewed monthly upon optional task being exercised	100% of VAMC listed optional tasks but be completed by go live, or within 12 months of optional task if no go live involved.
PWS 5.15.3 Optional Task: Remote Ad Hoc Training, Training Plan and Attendance Records	Training plan, attendance records, and quick reference guides for ad hoc training.	Prior to VAMC go live, or within 12 months of optional task if no go live involved.	Inspection by COR and VHA project management team	3 weeks Prior to each VAMC go live	100% of VAMC in scope of the project must receive the required training.
PWS 5.15.4 Optional Task: In Person Ad Hoc Training Plan and Records	Training plan, attendance records, and quick reference guides for ad hoc training.	Prior to VAMC go live, or within 12 months of optional task if no go live involved.	Inspection by COR and VHA project management team	3 weeks Prior to each VAMC go live	100% of VAMC in scope of the project must receive the required training.
PWS 5.15.5 Optional Task: FEHR Integration and Validation Checklist	FEHR integration and validation checklist per EHRM site transition outlining completed required testing activities.	Evaluation during each VAMC FEHR Go live	Inspection by COR and VHA project management team	Prior to each VAMC FEHR Go Live	100% of features and requirements must be implemented with the MTRS solution, as needed per EHRM transition.
PWS 5.15.5 Optional Task: Master Legacy and Delta Patient Lists	Master patient list and delta patient list to support transition from social security number to EDIPI.	Evaluation prior to each VAMC FEHR Go live. With master list due no more than 4 weeks before facility go live, and delta list within 5 days of the system cutover.	Inspection by COR and VHA project management team	2 months prior to VAMC FEHR go live and then weekly until cutover.	100% of VAMC in scope of the project that transition to FEHR must receive these services and support.

PWS Section/ Deliverable	Measurement/Metric	Deliverable Timeline	Method of Surveillance	Surveillance Frequency	Acceptable Quality Level (AQL)
PWS 5.15.6 Optional Task: AI Calculation Tool Model Requirements Document	Detailed description of data elements, modeling approach, algorithms, baseline assumptions	Within 1 month of optional task being exercised	Inspection by COR and VHA project management team	After 1 month of optional task being exercised	Document with 100% of modeling requirements topics included
PWS 5.15.6 Optional Task: AI Calculation Tool Model Development Package	Enterprise AI calculation tool license fully functional and ready for clinical use, implemented within the framework of the MTRS enterprise software.	Within 12 months of optional task being exercised.	Inspection by COR and VHA project management team	Reviewed monthly upon optional task being exercised. Sample size testing using 5 VAMCs.	Sample size testing of 5 VAMC must pass functionality test for AI calculation tool.
PWS 5.15.6 Optional Task: AI Calculation Tool Validation and Testing Report	Validation testing report showing AI calculation tool results for sample size of 20 individuals as identified by VA.	Within 12 months of optional task being exercised.	Inspection by COR and VHA project management team	Reviewed monthly upon optional task being exercised.	Clinical concurrence of sample size 5-year risk prediction tool.
PWS 5.15.6 Optional Task: AI Calculation Tool Technical Documentation Package	Package of technical documents including system architecture, data flow diagrams, operating procedures, and configuration management details.	Within 1 month of optional task being exercised	Inspection by COR and VHA project management team	After 1 month of optional task being exercised	100% of technical documents must be provided
PWS 5.15.6 Optional Task: AI Calculation Tool Training Package	Package of support documents including user guide, walkthroughs, and admin guide.	Within 1 month of optional task being exercised	Inspection by COR and VHA project management team	After 1 month of optional task being exercised	100% of training documents must be provided
PWS 5.15.6 Optional Task: AI Calculation Tool Monitoring and Change Management Plan	Semiannual review of AI model updates, model change management, recalibration, and performance reports.	Reviewed annually once option task is exercised	Inspection by COR and VHA project management team	Reviewed annually once option task is exercised	Action plan must include all required change management and performance details.

The COR will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable level of performance. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion. A Performance Based Service Assessment will be used by the COR in accordance with the QASP to assess Contractor performance.

6.5 FACILITY/RESOURCE PROVISIONS

The Contractor shall request other Government documentation deemed pertinent to the work accomplishment directly from the Government officials with whom the Contractor has contact. The Contractor shall consider the COR as the final source for needed Government documentation when the Contractor fails to secure the documents by other means. The Contractor is expected to use common knowledge and resourcefulness in securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

VA may provide remote access to VA specific systems/network in accordance with VA Handbook 6500, which requires the use of a VA approved method to connect external equipment/systems to VA's network. Citrix Access Gateway (CAG) and now the Azure Virtual Desktop (AVD) (as VA is currently transitioning from CAG to the AVD), are the current and only VA approved methods for remote access users when using or manipulating VA information for official VA Business. VA permits CAG remote access through approved Personally Owned Equipment (POE) and Other Equipment (OE), provided with the equipment meets all applicable 6500 Handbook requirements for POE/OE. All the security controls required for Government furnished equipment (GFE) must be utilized in approved POE or OE. The Contractor shall provide proof to the COR for review and approval that their POE or OE meets the VA Handbook 6500 requirements and VA Handbook 6500.6 Appendix C, herein incorporated as Addendum B, before use. CAG authorized users shall not be permitted to copy, print, or save any VA information accessed via CAG at any time. VA prohibits remote access to VA's network from non-North Atlantic Treaty Organization (NATO) countries. The exception to this are countries where VA has approved operations established (e.g. Philippines and South Korea). Exceptions are determined by the COR in coordination with the Information System Security Officer (ISSO) and Privacy Officer (PO).

This remote access may provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, PAL, Primavera, and Remedy, including appropriate seat management and user licenses, depending upon the level of access granted. The Contractor shall utilize government-provided software development and test accounts, documents, and requirements repositories, etc. as required for the development, storage, maintenance, and delivery of products within the scope of this effort. All VA sensitive information shall be protected at all times in accordance with VA Handbook 6500, local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. The Contractor shall ensure all work is performed in countries deemed not to pose a significant security risk. For detailed Security and Privacy Requirements (additional requirements of the contract consolidated into an addendum for easy reference) refer to **Error! Reference source not found.** and ADDENDUM B - VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE.

6.6 GOVERNMENT FURNISHED PROPERTY

No Government Furnished Equipment (GFE) will be provided as part of this contract.

6.7 SHIPMENT OF HARDWARE OR EQUIPMENT

There is no hardware or physical equipment being delivered within the scope of this contract.

7.0 POINTS OF CONTACT:

To Be Provided

8.0 ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

A1.0 Cyber and Information Security Requirements for VA IT Services

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations. The Contractor's firewall and web server shall meet or exceed VA minimum requirements for security. All VA data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer as soon as possible. The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to assessment and authorization and continuous monitoring.

Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before being placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, unless the connection uses FIPS 140-2 (or its successor) validated encryption, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The Contractor shall notify the COR/CO within one hour of disclosure or successful exploits of any vulnerability which can compromise the confidentiality, integrity, or availability of the information systems.

Each documented initiative under this contract incorporates VA Handbook 6500.6, "Contract Security," March 12, 2010 (Appendix C updated April 22, 2024) by reference as though fully set forth therein. The VA Handbook 6500.6, "Contract Security" shall also be included in every related agreement, contract, or order. The VA Handbook 6500.6, Appendix C, is included in this document as Addendum B.

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS) 2.0, and will be tracked therein. The TMS 2.0 may be accessed at https://www.tms.va.gov/SecureAuth35/. If you do not have a TMS 2.0 profile, go to https://www.tms.va.gov/SecureAuth35/ and click on the "Create New User" link on the TMS 2.0 to gain access.

Contractor employees shall complete a VA Systems Access Agreement if they are provided access privileges as an authorized user of the computer system of VA.

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with VA Enterprise Architecture (EA), available at http://www.ea.oit.va.gov/index.asp in force at the time of issuance of this contract, including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP). VA reserves the right to assess contract deliverables for EA compliance prior to acceptance.

A2.1. VA Internet and Intranet Standards

The Contractor shall adhere to and comply with VA Directive 6102 and VA's Web Governance if the Contractor's work includes building and maintaining VA's digital presence. This pertains, but is not limited to: websites, social media, creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=1056&FType=2

VA Web Governance website can be found at Home - VA Web Governance.

A3.0 Notice of the Federal Accessibility Law Affecting All Information and Communication Technology (ICT) Procurements (Section 508)

On January 18, 2017, the Access Board issued a final rule that updated accessibility requirements covered by Section 508 and refreshed guidelines for telecommunications equipment subject to Section 255 of the Communications Act. The final rule went into effect on January 18, 2018. The revisions and updates to the Section 508-based standards and Section 255-based guidelines are intended to ensure that information and communication technology (ICT) covered by the respective statutes is accessible to and usable by individuals with disabilities.

A3.1. Section 508 – Information and Communication Technology (ICT) Standards

The Section 508 standards established by the Access Board are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure ICT. These standards are found in their entirety at: Revised 508 Standards and 255 Guidelines (access-board.gov). A single PDF file version of the Revised Section 508 Standards and 255 Guidelines will be supplied upon request or can be obtained from the Access Board website. Federal agencies must comply with the Rehabilitation Act of 1973, as amended.

The Contractor shall comply with "508 Chapter 2: Scoping Requirements" for all electronic ICT and content delivered under this contract. Specifically, as appropriate for the technology and its functionality, the Contractor shall comply with the technical standards marked here:

☒ E205 Electronic Content – (Accessibility Standard -WCAG 2.0 Level A and AA Guidelines)
☒ E204 Functional Performance Criteria
☒ E206 Hardware Requirements
☒ E207 Software Requirements
☒ E208 Support Documentation and Services Requirements

A3.2. Compatibility with Assistive Technology

The standards do not require installation of specific accessibility-related software or attachment of an assistive technology device. Section 508 requires that ICT be compatible with such software and devices so that ICT can be accessible to and usable by individuals using assistive technology, including but not limited to screen readers, screen magnifiers, and speech recognition software.

A3.3. Acceptance and Acceptance Testing

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the Section 508 Chapter 2: Scoping Requirements standards identified above.

The Government reserves the right to test for Section 508 Compliance before delivery. The Contractor shall be able to demonstrate Section 508 Compliance upon delivery.

A4.0 Physical Security & Safety Requirements:

The Contractor and their personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property. Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed. It is the responsibility of the Contractor to park in the appropriate designated parking areas. VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

A5.0 Confidentiality and Non-Disclosure

The Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

The Contractor may have access to Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard (“Security Rule”). Pursuant to the Privacy and Security Rules, the

Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and ePHI.

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA CO will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA CO for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA CO.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
    a. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
    b. Controlled access to system and security software and documentation.
    c. Recording, monitoring, and control of passwords and privileges.
    d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
    e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.

   f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
   g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
   h. Contractor does not require access to classified data.
8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
9. VA Form 0752 shall be completed by all Contractor employees working on this contract and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

A6.0 Information Technology Using Sustainable Products

Not Applicable.

9.0 ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/ PRIVACY LANGUAGE

NOTE: In the event of a conflict, VA Acquisition Regulation (VAAR) Security Clauses take precedence over the language in this Addendum B.

APPLICABLE SECTIONS TAILORED FROM: *VA NOTICE 24-12, APRIL 22, 2024, UPDATE TO VA HANDBOOK 6500.6, CONTRACT SECURITY, APPENDIX C VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE, FOR INCLUSION INTO CONTRACTS, AS APPROPRIATE*

B1. GENERAL

This entire section applies to all acquisitions requiring any Information Security and Privacy language. Contractors, contractor personnel, Subcontractors and subcontractor personnel will be subject to the same federal laws, regulations, standards, VA directives and handbooks, as VA personnel regarding information and information system security and privacy.

B2. VA INFORMATION CUSTODIAL LANGUAGE

a. The Government shall receive unlimited rights to data/intellectual property first produced and delivered in the performance of this contract or order (hereinafter “contract”) unless expressly stated otherwise in this contract. This includes all rights to source code and all documentation created in support thereof. The primary clause used to define Government and Contractor data rights is FAR 52.227-14 Rights in Data – General.

b. Information made available to the Contractor by VA for the performance or administration of this contract will be used only for the purposes specified in the service agreement, SOW, PWS, PD, and/or contract. The Contractor shall not use VA information in any other manner without prior written approval from a VA Contracting Officer (CO). The primary clause used to define Government and Contractor data rights is FAR 52.227-14 Rights in Data – General.

c. VA information will not be co-mingled with any other data on the Contractor’s information systems or media storage systems. The Contractor shall ensure compliance with Federal and VA requirements related to data protection, data encryption, physical data segregation, logical data segregation, classification requirements and media sanitization.

d. VA reserves the right to conduct scheduled or unscheduled audits, assessments, or investigations of Contractor Information Technology (IT) resources to ensure information security is compliant with Federal and VA requirements. The Contractor shall provide all necessary access to records (including electronic and documentary materials related to the contracts and subcontracts) and support (including access to Contractor and Subcontractor staff associated with the contract) to VA, VA's Office Inspector General (OIG), and/or Government

Accountability Office (GAO) staff during periodic control assessments, audits, or investigations.

e. The Contractor may only use VA information within the terms of the contract and applicable Federal law, regulations, and VA policies. If new Federal information security laws, regulations or VA policies become applicable after execution of the contract, the parties agree to negotiate contract modification and adjustment necessary to implement the new laws, regulations, and/or policies.

f. The Contractor shall not make copies of VA information except as specifically authorized and necessary to perform the terms of the contract. If copies are made for restoration purposes, after the restoration is complete, the copies shall be destroyed in accordance with VA Directive 6500, VA Cybersecurity Program and VA Information Security Knowledge Service.

g. If a Veterans Health Administration (VHA) contract is terminated for default or cause with a business associate, the related local Business Associate Agreement (BAA) shall also be terminated and actions taken in accordance with VHA Directive 1605.05, Business Associate Agreements. If there is an executed national BAA associated with the contract, VA will determine what actions are appropriate and notify the contractor.

h. The Contractor shall store and transmit VA sensitive information in an encrypted form, using VA-approved encryption tools which are, at a minimum, Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules (or its successor) validated and in conformance with VA Information Security Knowledge Service requirements. The Contractor shall transmit VA sensitive information using VA approved Transport Layer Security (TLS) configured with FIPS based cipher suites in conformance with National Institute of Standards and Technology (NIST) 800-52, Guidelines for the Selection, Configuration and Use of Transport Layer Security (TLS) Implementations.

i. The Contractor’s firewall and web services security controls, as applicable, shall meet or exceed VA’s minimum requirements.

j. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor may use and disclose VA information only in two situations: (i) in response to a qualifying order of a court of competent jurisdiction after notification to VA CO (ii) with written approval from the VA CO. The Contractor shall refer all requests for, demands for production of or inquiries about, VA information and information systems to the VA CO for response.

k. Notwithstanding the provision above, the Contractor shall not release VA records protected by Title 38 U.S.C. § 5705, Confidentiality of medical quality-assurance records and/or Title 38 U.S.C. § 7332, Confidentiality of certain medical records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse or infection with Human Immunodeficiency Virus (HIV). If the Contractor is in receipt of a court order or other requests for the above-mentioned information, the

Contractor shall immediately refer such court order or other requests to the VA CO for response.

l. Information made available to the Contractor by VA for the performance or administration of this contract or information developed by the Contractor in performance or administration of the contract will be protected and secured in accordance with VA Directive 6500 and Identity and Access Management (IAM) Security processes specified in the VA Information Security Knowledge Service.

m. Any data destruction done on behalf of VA by a Contractor shall be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management, VA Handbook 6300.1, Records Management Procedures, and applicable VA Records Control Schedules.

n. The Contractor shall provide its plan for destruction of all VA data in its possession according to VA Directive 6500 and NIST 800-88, Guidelines for Media Sanitization prior to termination or completion of this contract. If directed by the COR/CO, the Contractor shall return all Federal Records to VA for disposition.

o. Any media, such as paper, magnetic tape, magnetic disks, solid state devices or optical discs that is used to store, process, or access VA information that cannot be destroyed shall be returned to VA. The Contractor shall hold the appropriate material until otherwise directed by the Contracting Officer's Representative (COR) or CO. Items shall be returned securely via VA-approved methods. VA sensitive information must be transmitted utilizing VA-approved encryption tools which are validated under FIPS 140-2 (or its successor) and NIST 800-52. If mailed, the Contractor shall send via a trackable method (USPS, UPS, FedEx, etc.) and immediately provide the COR/CO with the tracking information. Self-certification by the Contractor that the data destruction requirements above have been met shall be sent to the COR/CO within 30 business days of termination of the contract.

p. All electronic storage media (hard drives, optical disks, CDs, back-up tapes, etc.) used to store, process or access VA information will not be returned to the Contractor at the end of lease, loan, or trade-in. Exceptions to this paragraph will only be granted with the written approval of the VA CO.

B3. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees and subcontractors only to the extent necessary to perform the services specified in the solicitation or contract. This includes indirect entities, both affiliate of Contractor/Subcontractor and agent of Contractor/Subcontractor.

b. Contractors and subcontractors shall sign the VA Information Security Rule of Behavior (ROB) before access is provided to VA information and information

systems (see Section 4, Training, below). The ROB contains the minimum user compliance requirements and does not supersede any policies of VA facilities or other agency components which provide higher levels of protection to VA's information or information systems. Users who require privileged access shall complete the VA elevated privilege access request processes before privileged access is granted.

c. All Contractors and Subcontractors working with VA information are subject to the same security investigative and clearance requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors shall be in accordance with VA Directive and Handbook 0710, Personnel Vetting Program. The Office of Human Resources and Administration/Operations, Security and Preparedness (HRA/OSP) is responsible for these policies and procedures. Contract personnel who require access to classified information or information systems shall have an appropriate security clearance. Verification of a Security Clearance shall be processed through the Special Security Officer located in HRA/OSP. Contractors shall conform to all requirements stated in the National Industrial Security Program Operating Manual (NISPOM).

d. All Contractors and subcontractors shall comply with conditions specified in VAAR 852.204-71(d); Contractor operations required to be in United States. All Contractors and Subcontractors working with VA information must be permanently located within a jurisdiction subject to the law of the United States or its Territories to the maximum extent feasible. If services are proposed to be performed abroad the Contractor must state where all non-U.S. services are provided. The Contractor shall deliver to VA a detailed plan specifically addressing communications, personnel control, data protection and potential legal issues. The plan shall be approved by the COR/CO in writing prior to access being granted.

e. The Contractor shall notify the COR/CO in writing immediately (no later than 24 hours) after personnel separation or occurrence of other causes. Causes may include the following:
    (1) Contractor/Subcontractor personnel no longer has a need for access to VA information or VA information systems.

    (2) Contractor/Subcontractor personnel are terminated, suspended, or otherwise has their work on a VA project discontinued for any reason.

    (3) Contractor believes their own personnel or Subcontractor personnel may pose a threat to their company's working environment or to any company-owned property. This includes Contractor-owned assets, buildings, confidential data, customers, employees, networks, systems, trade secrets and/or VA data.

    (4) Any previously undisclosed changes to Contractor/Subcontractor background history are brought to light, including but not limited to changes to background investigation or employee record.

(5) Contractor/Subcontractor personnel have their authorization to work in the United States revoked.

(6) Agreement by which Contractor provides products and services to VA has either been fulfilled or terminated, such that VA can cut off electronic and/or physical access for Contractor personnel.

f. In such cases of contract fulfillment, termination, or other causes; the Contractor shall take the necessary measures to immediately revoke access to VA network, property, information, and information systems (logical and physical) by Contractor/Subcontractor personnel. These measures include (but are not limited to): removing and then securing Personal Identity Verification (PIV) badges and PIV – Interoperable (PIV-I) access badges, VA-issued photo badges, credentials for VA facilities and devices, VA-issued laptops, and authentication tokens. Contractors shall notify the appropriate VA COR/CO immediately to initiate access removal.

g. Contractors/Subcontractors who no longer require VA accesses will return VA-issued property to VA. This property includes (but is not limited to): documents, electronic equipment, keys, and parking passes. PIV and PIV-I access badges shall be returned to the nearest VA PIV Badge Issuance Office. Once they have had access to VA information, information systems, networks and VA property in their possessions removed, Contractors shall notify the appropriate VA COR/CO.

B4. TRAINING

a. All contractors and subcontractors requiring access to VA information and VA information systems shall successfully complete the following before being granted access to VA information and its systems:

(1) VA Privacy and Information Security Awareness and Rules of Behavior course (Talent Management System (TMS) #10176) initially and annually thereafter.

(2) Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the Organizational Rules of Behavior, relating to access to VA information and information systems initially and annually thereafter; and

(3) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system or information access [to be defined by the VA program official and provided to the VA CO for inclusion in the solicitation document – i.e., any role-based information security training].

b. The Contractor shall provide to the COR/CO a copy of the training certificates and certification of signing the Organizational Rules of Behavior for each

applicable employee within five days of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the required training is complete.

B5. SECURITY INCIDENT INVESTIGATION

a. The Contractor, Subcontractor, their employees, or business associates shall immediately (within one hour) report suspected security / privacy incidents to the VA OIT's Enterprise Service Desk (ESD) by calling (855) 673-4357 (TTY: 711). The ESD is OIT's 24/7/365 single point of contact for IT-related issues. After reporting to the ESD, the Contractor, Subcontractor, their employees, or business associates shall, within one hour, provide the COR/CO the incident number received from the ESD.

b. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor's notice to VA shall identify the information involved and the circumstances surrounding the incident, including the following:

    (1) The date and time (or approximation of) the Security Incident occurred.

    (2) The names of individuals involved (when applicable).

    (3) The physical and logical (if applicable) location of the incident.

    (4) Why the Security Incident took place (i.e., catalyst for the failure).

    (5) The amount of data belonging to VA believed to have been compromised.

    (6) The remediation measures the Contractor is taking to ensure no future incidents of a similar nature.

c. After the Contractor has provided the initial detailed incident summary to VA, they will continue to provide written updates on any new and relevant circumstances or facts they discover. The Contractor, Subcontractor, and their employes shall fully cooperate with VA or third-party entity performing an independent risk analysis on behalf of VA. Failure to cooperate may be deemed a material breach and grounds for contract termination.

d. VA IT Contractors shall follow VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program, and VA Information Security Knowledge Service guidance for implementing an Incident Response Plan or integrating with an existing VA implementation.

e. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG, and the

VA Office of Security and Law Enforcement. The Contractor, its employees, and its Subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/Subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

f. The Contractor shall comply with VA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information, which establishes the breach management policies and assigns responsibilities for the oversight, management and reporting procedures associated with managing of breaches.

g. With respect to unsecured Protected Health Information (PHI), the Contractor is deemed to have discovered a data breach when the Contractor knew or should have known of breach of such information. When a business associate is part of VHA contract, notification to the covered entity (VHA) shall be made in accordance with the executed BAA.

h. If the Contractor or any of its agents fails to protect VA sensitive personal information or otherwise engages in conduct which results in a data breach involving any VA sensitive personal information the Contractor/Subcontractor processes or maintains under the contract; the Contractor shall pay liquidated damages to the VA as set forth in clause 852.211-76, Liquidated Damages—Reimbursement for Data Breach Costs.

B6. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

a. Information systems designed or developed on behalf of VA at non-VA facilities shall comply with all applicable Federal law, regulations, and VA policies. This includes standards for the protection of electronic Protected Health Information (PHI), outlined in 45 C.F.R. Part 164, Subpart C and information and system security categorization level designations in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems and FIPS 200, Minimum Security Requirements for Federal Information Systems. Baseline security controls shall be implemented commensurate with the FIPS 199 system security categorization (reference VA Handbook 6500 and VA Trusted Internet Connections (TIC) Architecture).

b. Contracted new developments require creation, testing, evaluation, and authorization in compliance with VA Assessment and Authorization (A&A) processes in VA Handbook 6500 and VA Information Security Knowledge Service to obtain an Authority to Operate (ATO). VA Directive 6517, Risk Management Framework for Cloud Computing Services, provides the security and privacy requirements for cloud environments.

c. VA IT Contractors, Subcontractors and third-party service providers shall address and/or integrate applicable VA Handbook 6500, VA Handbook 6517, Risk

Management Framework for Cloud Computing Services and Information Security Knowledge Service specifications in delivered IT systems/solutions, products and/or services. If systems/solutions, products and/or services do not directly match VA security requirements, the Contractor shall work though the COR/CO to identify the VA organization responsible for governance or resolution. Contractors shall comply with FAR 39.1, specifically the prohibitions referenced.

d. The Contractor (including producers and resellers) shall comply with Office of Management and Budget (OMB) M-26-05 when using third-party software on VA information systems or otherwise affecting the VA information. This includes new software purchases and software renewals for software developed or modified by major version change. The term “software” includes firmware, operating systems, applications and application services (e.g., cloud-based software), as well as products containing software. The Contractor shall provide a self-attestation that secure software development practices are utilized as outlined by Executive Order (EO)14028 and NIST Guidance. A third-party assessment provided by either a certified Federal Risk and Authorization Management Program (FedRAMP) Third Party Assessor Organization (3PAO) or one approved by the agency will be acceptable in lieu of a software producer's self-attestation.

e. The Contractor shall ensure all delivered applications, systems and information systems are compliant with Homeland Security Presidential Directive (HSPD) 12 and VA Identity and Access management (IAM) enterprise identity management requirements as set forth in OMB M-19-17, M-05-24, FIPS 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors (or its successor), M-21-31 and supporting NIST guidance. This applies to Commercial Off-The-Shelf (COTS) product(s) that the Contractor did not develop, all software configurations and all customizations.

f. The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with VA Handbook 6500, VA Information Security Knowledge Service, IAM enterprise requirements and NIST 800-63, Digital Identity Guidelines, for direct, assertion-based authentication and/or trust-based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of PIV and/or Common Access Card (CAC), as determined by the business need and compliance with VA Information Security Knowledge Service specifications.

g. The Contractor shall use VA authorized technical security baseline configurations and certify to the COR that applications are fully functional and operate correctly as intended on systems in compliance with VA baselines prior to acceptance or connection into an authorized VA computing environment. If the Defense Information Systems Agency (DISA) has created a Security Technical Implementation Guide (STIG) for the technology, the Contractor may configure to comply with that STIG. If VA determines a new or updated VA configuration baseline needs to be created, the Contractor shall provide required technical support to develop the configuration settings. FAR 39.1 requires the population of

operating systems and applications includes all listed on the NIST National Checklist Program Checklist Repository,

h. The standard installation, operation, maintenance, updating and patching of software shall not alter the configuration settings from VA approved baseline configuration. Software developed for VA must be compatible with VA enterprise installer services and install to the default “program files” directory with silently install and uninstall. The Contractor shall perform testing of all updates and patching prior to implementation on VA systems.

i. Applications designed for normal end users will run in the standard user context without elevated system administration privileges.

j. The Contractor-delivered solutions shall reside on VA approved operating systems. Exceptions to this will only be granted with the written approval of the COR/CO.

k. The Contractor shall design, develop, and implement security and privacy controls in accordance with the provisions of VA security system development life cycle outlined in NIST 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, VA Directive and Handbook 6500, and VA Handbook 6517.

l. The Contractor shall comply with the Privacy Act of1974 (the Act), FAR 52.224-2 Privacy Act, and VA rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish a VA function.

m. The Contractor shall ensure the security of all procured or developed information systems, systems, major applications, minor applications, enclaves and platform information technologies, including their subcomponents (hereinafter referred to as “Information Systems”) throughout the life of this contract and any extension, warranty, or maintenance periods. This includes security configurations, workarounds, patches, hotfixes, upgrades, replacements and any physical components which may be necessary to remediate all security vulnerabilities published or known to the Contractor anywhere in the information systems (including systems, operating systems, products, hardware, software, applications and firmware). The Contractor shall ensure security fixes do not negatively impact the Information Systems.

n. When the Contractor is responsible for operations or maintenance of the systems, the Contractor shall apply the security fixes within the timeframe specified by the associated controls on the VA Information Security Knowledge Service. When security fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the Contractor shall provide written notice to the VA COR/CO that the patch has been validated as to not affecting the Systems within 10 business days.

B7. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE OR USE

a. The Contractor shall comply with all Federal laws, regulations, and VA policies for Information systems (cloud and non-cloud) that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities. Security controls for collecting, processing, transmitting, and storing of VA sensitive information, must be in place. The controls will be tested by VA or a VA sanctioned 3PAO and approved by VA prior to hosting, operation, maintenance or use of the information system or systems by or on behalf of VA. This includes conducting compliance risk assessments, security architecture analysis, routine vulnerability scanning, system patching, change management procedures and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures shall be the same as procedures used to secure VA-operated information systems.

b. Outsourcing (Contractor facility, equipment, or staff) of systems or network operations, telecommunications services or other managed services require Assessment and Authorization (A&A) of the Contractor's systems in accordance with VA Handbook 6500 as specified in VA Information Security Knowledge Service. Major changes to the A&A package may require reviewing and updating all the documentation associated with the change. The Contractor's cloud computing systems shall comply with FedRAMP and VA Directive 6517 requirements.

c. The Contractor shall return all electronic storage media (hard drives, optical disks, CDs, back-up tapes, etc.) on non-VA leased or non-VA owned IT equipment used to store, process or access VA information to VA in accordance with A&A package requirements. This applies when the contract is terminated or completed and prior to disposal of media. The Contractor shall provide its plan for destruction of all VA data in its possession according to VA Information Security Knowledge Service requirements and NIST 800-88. The Contractor shall send a self-certification that the data destruction requirements above have been met to the COR/CO within 30 business days of termination of the contract.

d. All external internet connections to VA network involving VA information must be in accordance with VA Trusted Internet Connection (TIC) Reference Architecture and VA Directive and Handbook 6513, Secure External Connections and reviewed and approved by VA prior to implementation. Government-owned Contractor-operated systems, third party or business partner networks require a Memorandum of Understanding (MOU) and Interconnection Security Agreements (ISA).

e. Contractor procedures shall be subject to periodic, announced, or unannounced assessments by VA officials, the OIG or a 3PAO. The physical security aspects associated with Contractor activities are also subject to such assessments. The Contractor shall report, in writing, any deficiencies noted during the above assessment to the VA COR/CO. The Contractor shall use VA's defined processes to document planned remedial actions that address identified deficiencies in information security policies, procedures, and practices. The

Contractor shall correct security deficiencies within the timeframes specified in the VA Information Security Knowledge Service.

f. All major information system changes which occur in the production environment shall be reviewed by the VA to determine the impact on privacy and security of the system. Based on the review results, updates to the Authority to Operate (ATO) documentation and parameters may be required to remain in compliance with VA Handbook 6500 and VA Information Security Knowledge Service requirements.

g. The Contractor shall conduct an annual privacy and security self-assessment on all information systems and outsourced services as required. Copies of the assessment shall be provided to the COR/CO. The VA/Government reserves the right to conduct assessment using government personnel or a third-party if deemed necessary. The Contractor shall correct or mitigate any weaknesses discovered during the assessment.

h. VA prohibits the installation and use of personally owned or Contractor-owned equipment or software on VA information systems. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW, PWS, PD or contract. All security controls required for government furnished equipment must be utilized in VA approved Other Equipment (OE). Configuration changes to the Contractor OE, must be funded by the owner of the equipment. All remote systems must use a VA-approved antivirus software and a personal (host-based or enclave based) firewall with a VA-approved configuration. The Contractor shall ensure software on OE is kept current with all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-virus software and the firewall on the non-VA owned OE. Approved Contractor OE will be subject to technical inspection at any time.

i. The Contractor shall notify the COR/CO within one hour of disclosure or successful exploits of any vulnerability which can compromise the confidentiality, integrity, or availability of the information systems. The system or effected component(s) need(s) to be isolated from the network. A forensic analysis needs to be conducted jointly with VA. Such issues will be remediated as quickly as practicable, but in no event longer than the timeframe specified by VA Information Security Knowledge Service. If sensitive personal information is compromised reference VA Handbook 6500.2 and Section 5, Security Incident Investigation.

j. For cases wherein the Contractor discovers material defects or vulnerabilities impacting products and services they provide to VA, the Contractor shall develop and implement policies and procedures for disclosure to VA, as well as remediation. The Contractor shall, within 30 business days of discovery, document a summary of these vulnerabilities or defects. The documentation will include a description of the potential impact of each vulnerability and material defect, compensating security controls, mitigations, recommended corrective actions, root cause analysis and/or workarounds (i.e., monitoring). Should there

exist any backdoors in the products or services they provide to VA (referring to methods for bypassing computer authentication), the Contractor shall provide the VA CO/CO written assurance they have permanently remediated these backdoors.

k. All other vulnerabilities, including those discovered through routine scans or other assessments, will be remediated based on risk, in accordance with the remediation timelines specified by the VA Information Security Knowledge Service and/or the applicable timeframe mandated by Cybersecurity & Infrastructure Security Agency (CISA) Binding Operational Directive (BOD) 22-01 and BOD 19-02 for Internet-accessible systems. Exceptions to this paragraph will only be granted with the approval of the COR/CO.

B8. SECURITY AND PRIVACY CONTROLS COMPLIANCE TESTING, ASSESSMENT AND AUDITING

a. Should VA request it, the Contractor shall provide a copy of their (corporation's, sole proprietorship's, partnership's, limited liability company (LLC), or other business structure entity's) policies, procedures, evidence and independent report summaries related to specified cybersecurity frameworks (International Organization for Standardization (ISO), NIST Cybersecurity Framework (CSF), etc.). VA or its third-party/partner designee (if applicable) are further entitled to perform their own audits and security/penetration tests of the Contractor's IT or systems and controls, to ascertain whether the Contractor is complying with the information security, network or system requirements mandated in the agreement between VA and the Contractor.

b. Any audits or tests of the Contractor or third-party designees/partner VA elects to carry out will commence within 30 business days of VA notification. Such audits, tests and assessments may include the following: (a): security/penetration tests which both sides agree will not unduly impact Contractor operations; (b): interviews with pertinent stakeholders and practitioners; (c): document review; and (d): technical inspections of networks and systems the Contractor uses to destroy, maintain, receive, retain, or use VA information.

c. As part of these audits, tests and assessments, the Contractor shall provide all information requested by VA. This information includes, but is not limited to, the following: equipment lists, network or infrastructure diagrams, relevant policy documents, system logs or details on information systems accessing, transporting, or processing VA data.

d. The Contractor and at its own expense, shall comply with any recommendations resulting from VA audits, inspections and tests. VA further retains the right to view any related security reports the Contractor has generated as part of its own security assessment. The Contractor shall also notify VA of the existence of any such security reports or other related assessments, upon completion and validation.

e. VA appointed auditors or other government agency partners may be granted access to such documentation on a need-to-know basis and coordinated through the COR/CO. The Contractor shall comply with recommendations which result from these regulatory assessments on the part of VA regulators and associated government agency partners.

B9. PRODUCT INTEGRITY, AUTHENTICITY, PROVENANCE, ANTI-COUNTERFEIT AND ANTI-TAMPERING

a. The Contractor shall comply with Code of Federal Regulations (CFR) Title 15 Part 7, “Securing the Information and Communications Technology and Services (ICTS) Supply Chain”, which prohibits ICTS Transactions from foreign adversaries. ICTS Transactions are defined as any acquisition, importation, transfer, installation, dealing in or use of any information and communications technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs or the platforming or data hosting of applications for consumer download.

b. When contracting terms require the Contractor to procure equipment, the Contractor shall purchase or acquire the equipment from an Original Equipment Manufacturer (OEM) or an authorized reseller of the OEM. The Contractor shall attest that equipment procured from an OEM or authorized reseller or distributor are authentic. If procurement is unavailable from an OEM or authorized reseller, the Contractor shall submit in writing, details of the circumstances prohibiting this from happening and procure a product waiver from the VA COR/CO.

c. All Contractors shall establish, implement, and provide documentation for risk management practices for supply chain delivery of hardware, software (to include patches) and firmware provided under this agreement. Documentation will include chain of custody practices, inventory management program, information protection practices, integrity management program for sub-supplier provided components, and replacement parts requests. The Contractor shall make spare parts available. All Contractor(s) shall specify how digital delivery for procured products, including patches, will be validated and monitored to ensure consistent delivery. The Contractor shall apply encryption technology to protect procured products throughout the delivery process.

d. If a Contractor provides software or patches to VA, the Contractor shall publish or provide a hash conforming to the FIPS Security Requirements for Cryptographic Modules (FIPS 140-2 or successor).

e. The Contractor shall provide a software bill of materials (SBOM) for procured (to include licensed products) and consist of a list of components and associated metadata which make up the product. SBOMs must be generated in one of the data formats defined in the National Telecommunications and Information Administration (NTIA) report “The Minimum Elements for a Software Bill of Materials (SBOM).”

f. Contractors shall use or arrange for the use of trusted channels to ship procured products, such as U.S. registered mail and/or tamper-evident packaging for physical deliveries.

g. Throughout the delivery process, the Contractor shall demonstrate a capability for detecting unauthorized access (tampering).

h. The Contractor shall demonstrate chain-of-custody documentation for procured products and require tamper-evident packaging for the delivery of this hardware.

B10. VIRUSES, FIRMWARE, AND MALWARE

a. The Contractor shall execute due diligence to ensure all provided software and patches, including third-party patches, are free of viruses and/or malware before releasing them to or installing them on VA information systems.

b. The Contractor warrants it has no knowledge of and did not insert, any malicious virus and/or malware code into any software or patches provided to VA which could potentially harm or disrupt VA information systems. The Contractor shall use due diligence, if supplying third-party software or patches, to ensure the third-party has not inserted any malicious code and/or virus which could damage or disrupt VA information systems.

c. The Contractor shall provide or arrange for the provision of technical justification as to why any “false positive” hit has taken place to ensure their code’s supply chain has not been compromised. Justification may be required, but is not limited to, when install files, scripts, firmware, or other Contractor-delivered software solutions (including third-party install files, scripts, firmware, or other software) are flagged as malicious, infected, or suspicious by an anti-virus vendor.

d. The Contractor shall not upload (intentionally or negligently) any virus, worm, malware or any harmful or malicious content, component and/or corrupted data/source code (hereinafter “virus or other malware”) onto VA computer and information systems and/or networks. If introduced (and this clause is violated), upon written request from the VA CO, the Contractor shall:

(1) Take all necessary action to correct the incident, to include any and all assistance to VA to eliminate the virus or other malware throughout VA’s information networks, computer systems and information systems; and
(2) Use commercially reasonable efforts to restore operational efficiency and remediate damages due to data loss or data integrity damage, if the virus or other malware causes a loss of operational efficiency, data loss, or damage to data integrity.

B11. CRYPTOGRAPHIC REQUIREMENT

a. The Contractor shall document how the cryptographic system supporting the Contractor’s products and/or services protect the confidentiality, data integrity,

authentication and non-repudiation of devices and data flows in the underlying system.

b. The Contractor shall use only approved cryptographic methods as defined in FIPS 140-2 (or its successor) and NIST 800-52 standards when enabling encryption on its products.

c. The Contractor shall provide or arrange for the provision of an automated remote key-establishment method which protects the confidentiality and integrity of the cryptographic keys.

d. The Contractor shall ensure emergency re-keying of all devices can be remotely performed within 30 business days.

e. The Contractor shall provide or arrange for the provision of a method for updating cryptographic primitives or algorithms.

B12. PATCHING GOVERNANCE

a. The Contractor shall provide documentation detailing the patch management, vulnerability management, mitigation and update processes (to include third-party) prior to the connection of electronic devices, assets or equipment to VA's assets. This documentation will include information regarding the following:

    (1) The resources and technical capabilities to sustain the program or process (e.g., how the integrity of a patch is validated by VA); and.

    (2) The approach and capability to remediate newly reported zero-day vulnerabilities for Contractor products.

b. The Contractor shall verify and provide documentation all procured products (including third-party applications, hardware, software, operating systems, and firmware) have appropriate updates and patches installed prior to delivery to VA.

c. The Contractor shall provide or arrange the provision of appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses for their products and services within 30 days of discovery. Updates to remediate critical or emergent vulnerabilities will be provided within seven business days of discovery. If updates cannot be made available by Contractor within these time periods, the Contractor shall submit mitigations, methods of exploit detection and/or workarounds to the COR/CO prior to the above deadlines.

d. The Contractor shall provide or arrange for the provision of appropriate hardware, software and/or firmware updates, when those products, including open-source software, are provided to the VA, to remediate newly discovered vulnerabilities or weaknesses. Remediations of products or services provided to the VA's system environment must be provided within 30 business days of availability from the original supplier and/or patching source. Updates to remediate critical vulnerabilities applicable to the Contractor's use of the third-

party product in its system environment will be provided within seven business days of availability from the original supplier and/or patching source. If applicable third-party updates cannot be integrated, tested and made available by Contractor within these time periods, mitigations and/or workarounds will be provided to the COR/CO before the above deadlines.

B13. SPECIALIZED DEVICES/SYSTEMS (MEDICAL DEVICES, SPECIAL PURPOSE SYSTEMS, RESEARCH SCIENTIFIC COMPUTING)

a. Contractor supplies/delivered Medical Devices, Special Purpose Systems-Operational Technology (SPS-OT) and Research Scientific Computing Devices shall comply with all applicable Federal law, regulations, and VA policies. New developments require creation, testing, evaluation, and authorization in compliance with processes specified on the Specialized Device Cybersecurity Department Enterprise Risk Management (SDCD-ERM) Portal, VA Directive 6550, Pre-Procurement Assessment and Implementation of Medical Devices/Systems, VA Handbook 6500, and the VA Information Security Knowledge Service. Deviations from Federal law, regulations, and VA Policy are identified and documented as part of VA Directive 6550 and/or the VA Enterprise Risk Analysis (ERA) processes for Specialized Devices/Systems processes.

b. All Contractors and third-party service providers shall address and/or integrate applicable VA Handbook 6500 and Information Security Knowledge Service specifications in delivered IT systems/solutions, products and/or services. If systems/solutions, products and/or services do not directly match VA security requirements, the Contractor shall work though the COR/CO for governance or resolution.

c. The Contractor shall certify to the COR/CO that devices/systems that have completed the VA Enterprise Risk Analysis (ERA) process for Specialized Devices/Systems are fully functional and operate correctly as intended. Devices/systems must follow the VA ERA authorized configuration prior to acquisition and connection to the VA computing environment. If VA determines a new VA ERA needs to be created, the Contractor shall provide required technical support to develop the configuration settings. Major changes to a previously approved device/system will require a new ERA.

d. The Contractor shall comply with all practices documented by the Food Drug and Administration (FDA) Premarket Submission for Management of Cybersecurity in Medical Devices and Postmarket Management of Cybersecurity in Medical Devices.

e. The Contractor shall design devices capable of accepting all applicable security patches with or without the support of the Contractor personnel. If patching can only be completed by the Contractor, the Contractor shall commit the resources needed to patch all applicable devices at all VA locations. If unique patching instructions or packaging is needed, the Contractor shall provide the necessary information in conjunction with the validation/testing of the patch. The Contractor shall apply security patches within 30 business days of the patch release and

have a formal tracking process for any security patches not implemented to include explanation when a device cannot be patched.

f. The Contractor shall provide devices able to install and maintain VA-approved antivirus capabilities with the capability to quarantine files and be updated as needed in response to incidents. Alternatively, a VA-approved whitelisting application may be used when the Contractor cannot install an anti-virus / anti-malware application.

g. The Contractor shall verify and document all software embedded within the device does not contain any known viruses or malware before delivery to or installation at a VA location.

h. Devices and other equipment or systems containing media (hard drives, optical disks, solid state, and storage via chips/firmware) with VA sensitive information will be returned to the Contractor with media removed. When the contract requires return of equipment, the options available to the Contractor are the following:

(1) The Contractor shall accept the system without the drive, firmware and solid state.

(2) VA's initial device purchase includes a spare drive or other replacement media which must be installed in place of the original drive at time of turn-in; or

(3) Due to the highly specialized and sometimes proprietary hardware and software associated with the device, if it is not possible for VA to retain the hard drive, firmware, and solid state, then:

(a) The equipment Contractor shall have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact.

(b) Any fixed hard drive, Complementary Metal-Oxide-Semiconductor (CMOS), Programmable Read-Only Memory (PROM), solid state and firmware on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be pre-approved and described in the solicitation, contract, or order.

B14. DATA CENTER PROVISIONS

1. The Contractor shall ensure the VA network is accessed by in accordance with VA Directive 6500 and IAM security processes specified in the VA Information Security Knowledge Service.

2. The Contractor shall ensure network infrastructure and data availability in accordance with VA information system business continuity procedures specified in the VA Information Security Knowledge Service.

3. The Contractor shall ensure any connections to the internet or other external networks for information systems occur through managed interfaces utilizing VA approved boundary protection devices (e.g., internet proxies, gateways, routers, firewalls, guards or encrypted tunnels).

4. The Contractor shall encrypt all traffic across the segment of the Wide Area Network (WAN) it manages and no unencrypted Out of Band (OOB) Internet Protocol (IP) traffic will traverse the network.

5. The Contractor shall ensure tunnel endpoints are routable addresses at each VA operating site.

6. The Contractor shall secure access from Local Area Networks (LANs) at co-located sites in accordance with VA TIC Reference Architecture, VA Directive and Handbook 6513, and MOU/ISA process specified in the VA Information Security Knowledge Service.

10.0 ADDENDUM C – VAMC FACILITIES

10.1 Base Period:

The contractor shall deliver MTRS services to the following 30 VA Medical Center (VAMC) facilities within 12 months after acceptance of order.

MAP_ID	Station #	FACILITY	CITY	STATE	MTRS
11072	526	James J. Peters VAMC	Bronx	NY	MagView
11457	528	Buffalo VAMC	Buffalo	NY	Volpara - Patient Hub
9433	528A8	Samuel S. Stratton VAMC	Albany	NY	Volpara - MRS
11289	630	VA NY Harbor Healthcare-Manhattan Campus -VHA	New York	NY	Volpara - Patient Hub
12001	630A4	VA NY Harbor Healthcare Sys.-Brooklyn Campus- VHA	Brooklyn	NY	Volpara - Patient Hub
17184	540	Louis A Johnson VAMC - VHA	Clarksburg	WV	MagView
10909	516	C.W. Bill Young Dept. of VAMC	Bay Pines	FL	Volpara - Patient Hub
50165	516BZ	Lee County VA Clinic - VHA	Cape Coral	FL	Volpara - Patient Hub
11274	546	Bruce W. Carter Dept of VAMC	Miami	FL	MagView
17218	546	William Bill Kling VA OP Clinic - VHA	Sunrise	FL	MagView
11410	548	West Palm Beach VAMC	West Palm Beach	FL	Volpara - Patient Hub
50569	573	Malcom Randall VA Medical Center - VHA	Gainesville	FL	Volpara - Patient Hub
60633	573BY	Jacksonville North VA Clinic	Jacksonville	FL	Volpara - Patient Hub
50194	573BY	Jacksonville VA Outpatient Clinic - VHA	Jacksonville	FL	Volpara - Patient Hub
17858	672	VA Caribbean Health Care System - VHA	San Juan	PR	Volpara - Patient Hub
9855	673	James A. Haley Veterans Administration Hospital-VHA	Tampa	FL	Volpara - Patient Hub
60694	673GB	Lakeland VA Clinic - VHA	Lakeland	FL	Volpara - Patient Hub
60514	673QJ	Hidden River VA Clinic- VHA	Tampa	FL	Volpara - Patient Hub
18023	673BZ	James A Haley Veterans Hosp New Port Richey OPC-VHA	New Port Richey	FL	Volpara - Patient Hub
60230	635	Oklahoma City VAMC	Oklahoma City	OK	MagView
60158	6402	Ernest Childers VA Outpatient Clinic	Tulsa	OK	MagView
10769	600	VA Long Beach Healthcare System- VHA	Long Beach	CA	MagView
14017	605	VA Loma Linda Healthcare-VHA	Loma Linda	CA	Volpara - Patient Hub
10737	644	Phoenix VA Health Care System - VHA	Phoenix	AZ	MagView
10672	664	VA San Diego Healthcare System- VHA	San Diego	CA	MagView
10987	678	Southern Arizona VA Healthcare System- VHA	Tucson	AZ	Volpara - Patient Hub
11213	691	VA Greater L.A. Healthcare System - VHA	Los Angeles	CA	NONE - Award Pending

MAP_ID	Station #	FACILITY	CITY	STATE	MTRS
50214	618	Minneapolis VA Healthcare System - VHA	Minneapolis	MN	MagView
17336	691A4	VA Greater L.A. Healthcare Sys. VHA Sepulveda - VHA	North Hills	CA	NONE – Award Pending
17639	605BZ	VA Loma Linda Ambulatory Care Center	Redlands (605=Loma Linda)	CA	Volpara - Patient Hub

10.2 Optional Task 1:

The Contractor shall deliver the MTRS solution to all 78 VA Medical Center (VAMC) facilities within 12 months of modification acceptance. Delivery details for 58 facilities are provided in the chart below. The remaining 20 facility locations will be identified and provided at the time the option is exercised.

MAP_ID	Station #	FACILITY	CITY	STATE	MTRS
13515	523	Boston VA Healthcare System Mammography Dept -VHA	Boston	MA	Volpara - Patient Hub
60129	593	Wilkes-Barre VAMC	Wilkes-Barre	PA	Volpara - Patient Hub
8814	642	Corporal Michael J. Crescenz VAMC - VHA	Philadelphia	PA	Volpara - Patient Hub
17288	646	VA Pittsburgh Healthcare System - VHA	Pittsburgh	PA	Volpara - Patient Hub
10657	512	Dept. of Veteran Affairs Medical Center - Baltimore- VHA	Baltimore	MD	MagView
11913	688	VAMC 114 - VHA	Washington	DC	MagView
11245	558	Durham VAMC - VHA	Durham	NC	Volpara - Patient Hub
50592	558G	Greenville VA Healthcare Center 558G - MOBILE	Greenville - Mobile	NC	Volpara - Patient Hub
60845	558GA	GREENVILLE VA HCC-VHA	Greenville	NC	Volpara - Patient Hub
50719	565	Cumberland County VA Clinic - VHA	Fayetteville	NC	Volpara - Patient Hub
17802	590	Hampton VAMC - VHA	Hampton	VA	Volpara - Patient Hub
12598	652	Richmond VAMC	Richmond	VA	Volpara - Patient Hub
60679	652	CVHCS Women's Health Center - RIC - VHA	Richmond	VA	Volpara - Patient Hub
10894	659	W.G. Hefner Salisbury VAMC	Salisbury	NC	Volpara - Patient Hub
51292	659BZ	South Charlotte VA Clinic	Charlotte	NC	Volpara - Patient Hub
TBD	508	Atlanta VA Medical Center	Atlanta	GA	Volpara – Patient Hub
51701	509	VA Augusta Health Care System	Augusta	GA	Volpara - Patient Hub
50712	521	Birmingham VA Clinic, Breast Imaging-VHA	Birmingham	AL	MagView
52196	521GA	Huntsville VA Clinic, Breast Imaging-VHA	Huntsville	AL	MagView
9872	544	Wm Jennings Bryan Dorn VAMC	Columbia	SC	Volpara - Patient Hub
14636	675	VIERA VA CLINIC	Viera	FL	Volpara - Patient Hub
12045	675GC	Lake Baldwin VAMC	Orlando	FL	Volpara - Patient Hub

MAP_ID	Station #	FACILITY	CITY	STATE	MTRS
50539	675GA	Orlando VAMC	Orlando	FL	Volpara - Patient Hub
50946	603	Robley Rex Veterans Medical Center-Newburg-VHA	Louisville	KY	Volpara - Patient Hub
11227	626	VA TN Valley Healthcare System Nashville Campus-VHA	Nashville	TN	Volpara - Patient Hub
11861	626A4	Alvin C. York VAMC - VHA	Murfreesboro	TN	Volpara - Patient Hub
11340	541	VA Northeast Ohio Healthcare System	Cleveland	OH	Volpara - Patient Hub
60369	541BY	VANEOHS Mobile Mammography-VHA Mobile	Canton	OH	Volpara - Patient Hub
17586	556	Captain James A Lovell IL VAMC	North Chicago	IL	Volpara - Patient Hub
60187	589Af	Harry S. Truman Memorial Veterans' Hospital	Columbia	MO	Volpara - Patient Hub
11138	657	John Cochran Memorial Hospital - VHA	St. Louis	MO	Volpara - MRS
11288	580	Michael E. DeBakey VAMC	Houston	TX	Volpara - Patient Hub
11015	598	Central Arkansas Health Care System - Little Rock	Little Rock	AR	Volpara - Patient Hub
10997	549	Veterans Affairs North Texas Health Care System-VHA	Dallas	TX	MagView
17652	549BY	Veterans Affairs Fort Worth OP Clinic-VHA	Fort Worth	TX	MagView
9101	671	Audie L. Murphy Memorial Hospital	San Antonio	TX	Volpara - Patient Hub
52163	671GS	Northwest San Antonio VA Clinic	San Antonio	TX	Volpara - Patient Hub
16739	671G0	North Central Federal VA Clinic	San Antonio	TX	Volpara - Patient Hub
60405	671A4	Kerrville VAMC	Kerrville	TX	Volpara - Patient Hub
14067	674	Olin E. Teague Vet Center - VHA	Temple	TX	Volpara - Patient Hub
18219	674BY	Austin VA Clinic	Austin	TX	Volpara - Patient Hub
60175	740GC	Corpus Christi West Point CLIN	Corpus Christi (740=Harlingen)	TX	Volpara - Patient Hub
51514	740GB	McAllen OPC - VHA	McAllen (740=Harlingen)	TX	Volpara - Patient Hub
17067	459	Spark M Matsunaga Med Center - VHA	Honolulu	HI	Volpara - MRS
15122	593	Southern Nevada HCS	North Las Vegas	NV	Volpara - MRS
8860	612	Martinez VAMC	Martinez	CA	Volpara - Patient Hub
14361	612	Sacramento VA Medical Center	Mather	CA	Volpara - Patient Hub
8376	612GH	McClellan VA Clinic	McClellan	CA	Volpara - Patient Hub
60506	612QE	Richard A. Pittman VA Clinic	French Camp	CA	Volpara - Patient Hub
18082	612B4	Redding VA Clinic	Redding	CA	Volpara - Patient Hub
51195	640	VA Palo Alto Health Care System - VHA	Palo Alto	CA	MagView
52135	640HC	VAPAHCS Marina Outpatient Clinic - Mammography	Marina	CA	MagView
8385	501	Raymond G Murphy VAMC - VHA	Albuquerque	NM	MagView

MAP_ID	Station #	FACILITY	CITY	STATE	MTRS
50390	636A6	VA Central Iowa Healthcare System - VHA	Des Moines	IA	Volpara - Patient Hub
50733	636A8	Iowa City VAMC - VHA	Iowa City	IA	Volpara - Patient Hub
TBD	660	George E Wahlen VAMC, Salt Lake City Utah	Salt Lake City	UT	New mammography program being developed, no existing solution in place
TBD	578	Edward Hines Jr. VAMC, Hines, IL	Hines	IL	New mammography program being developed, no existing solution in place
TBD	664	Jennifer Moreno VAMC, San Diego, CA	San Diego	CA	New mammography program being developed, no existing solution in place

SECTION C - CONTRACT CLAUSES

ADDENDUM to RFO 52.212-4 CONTRACT TERMS AND CONDITIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

Clauses that are incorporated by reference (by Citation Number, Title, and Date), have 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 following clauses are incorporated into 52.212-4 as an addendum to this contract:

C.1 RFO 52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (NOV 2020)

(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 Department of Veterans Affairs (VA) Acquisition Regulation (VAAR) (48 CFR Chapter 8) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of Clause)

C.2 RFO 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/far-overhaul/far-part-deviation-guide
https://www.va.gov/oal/library/vaar/

RFO / VAAR Clause Number	Title	Date
52.203-3	Gratuities	Apr 1984
52.203-6	Restrictions On Subcontractor Sales to the Government	Jun 2020
52.203-12	Limitation On Payments To Influence Certain Federal Transactions	JUN 2020
52.203-13	Contractor Code of Business Ethics and Conduct	Nov 2021
52.203-17	Contractor Employee Whistleblower Rights	Nov 2023
52.203-19	Prohibition On Requiring Certain Internal Confidentiality Agreements or Statements	Jan 2017
52.204-13	System For Award Management—Maintenance (Deviation)	Nov 2025
52.204-19	Incorporation By Reference of Representations and Certifications	Dec 2014

RFO / VAAR Clause Number	Title	Date
52.209-6	Protecting The Government's Interest When Subcontracting with Contractors Debarred, Suspended, Proposed for Debarment, Or Voluntarily Excluded (Deviation)	Nov 2025
52.209-9	Updates Of Publicly Available Information Regarding Responsibility Matters	Nov 2025
52.209-10	Prohibition On Contracting with Inverted Domestic Corporations	Nov 2015
52.212-4	Contract Terms and Conditions—Commercial Products and Commercial Services	Oct 2025
52.219-4	Notice Of Price Evaluation Preference For HubZone SBS	Oct 2022
52.219-9	Small Business Subcontracting Plan	NOV 2025
52.219-8	Utilization Of Small Business Concerns (Deviation)	Nov 2025
52.219-9	Small Business Subcontracting Plan (Deviation)	Nov 2025
52.219-28	Post Award Small Business Program Rerepresentation (Deviation)	Nov 2025
52.222-3	Convict Labor (Deviation)	Nov 2025
52.222-35	Equal Opportunity for Veterans (Deviation)	Nov 2025
52.222-36	Equal Opportunity for Workers with Disabilities (Deviation)	Nov 2025
52.222-37	Employment Reports on Veterans (Deviation)	Nov 2025
52.222-40	Notification Of Employee Rights Under the National Labor Relations Act (Deviation)	Nov 2025
52.222-50	Combating Trafficking in Persons (Deviation)	Nov 2025
52.223-23	Sustainable Products (Deviation)	Nov 2025
52.224-1	Privacy Act Notification	Apr 1984
52.224-2	Privacy Act	Apr 1984
52.224-3	Privacy Training	Jan 2017
52.226-8	Encouraging Contractor Policies to Ban Text Messaging While Driving	May 2024
52.227-1	Authorization And Consent	Jun 2020
52.227-2	Notice And Assistance Regarding Patent and Copyright Infringement	Jun 2020
52.227-14	Rights in Data General	May 2014
52.229-11	Tax on Certain Foreign Procurements—Notice and Representation (Deviation)	Sept 2025
52.229-12	Tax On Certain Foreign Procurements	Sept 2025
52.232-33	Payment By Electronic Funds Transfer—System for Award Management	Oct 2018
52.232-39	Unenforceability Of Unauthorized Obligations	Jun 2013
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	Mar 2023
52.233-1	Disputes	May 2014
52.233-3	Protest After Award	Aug 1996
52.233-4	Applicable Law for Breach of Contract Claim	OCT 2004

RFO / VAAR Clause Number	Title	Date
52.240-93	Basic Safeguarding of Covered Contractor Information Systems (Deviation)	Nov 2025
52.242-5	Payments To Small Business Subcontractors	Jan 2017
52.242-13	Bankruptcy	Jul 1995
852.201-70	Contracting Officer's Representative	Dec 2022
852.203-70	Commercial Advertising	May 2018
852.215-70	Service-Disabled Veteran-Owned and Veteran-Owned Small Business Evaluation Factors (Deviation)	Jan 2023
852.215-71	Evaluation Factor Commitments	Oct 2019
852.219-70	VA Small Business Subcontracting Plan Minimum Requirements	"JAN 2023
852.222-71	Compliance With Executive Order 13899 (Deviation) (Apr 2025)	Apr 2025
852.232-72	Electronic Submission of Payment Requests	Nov 2018
852.239-70	Security Requirements for Information Technology Resources	Feb 2023
852.239-72	Information System Design and Development	Feb 2023
852.239-73	Information System Hosting, Operation, Maintenance, Or Use	Feb 2023
852.239-74	Security Controls Compliance Testing	Feb 2023

(End of Clause)

C.3 RFO 52.203-12 LIMITATION ON PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS (JUN 2020)

(a) *Definitions.* As used in this clause—

Agency means "*executive agency*" as defined in Federal Acquisition Regulation (FAR) 2.101.

Covered Federal action means any of the following actions:
(1) Awarding any Federal contract.
(2) Making any Federal grant.
(3) Making any Federal loan.
(4) Entering into any cooperative agreement.
(5) Extending, continuing, renewing, amending, or modifying any Federal contract, grant, loan, or cooperative agreement.

Indian tribe and "tribal organization" have the meaning provided in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b) and include Alaskan Natives.

Influencing or attempting to influence means making, with the intent to influence, any communication to or appearance before an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any covered Federal action.

Local government means a unit of government in a State and, if chartered, established, or otherwise recognized by a State for the performance of a governmental duty, including a local public authority, a special district, an intrastate district, a council of governments, a sponsor group representative organization, and any other instrumentality of a local government.

Officer or employee of an agency includes the following individuals who are employed by an agency:

(1) An individual who is appointed to a position in the Government under Title 5, United States Code, including a position under a temporary appointment.
(2) A member of the uniformed services, as defined in subsection 101(3), Title 37, United States Code.
(3) A special Government employee, as defined in section 202, Title 18, United States Code.
(4) An individual who is a member of a Federal advisory committee, as defined by the Federal Advisory Committee Act, Title 5, United States Code, appendix 2.

Person means an individual, corporation, company, association, authority, firm, partnership, society, State, and local government, regardless of whether such entity is operated for profit, or not for profit. This term excludes an Indian tribe, tribal organization, or any other Indian organization eligible to receive Federal contracts, grants, cooperative agreements, or loans from an agency, but only with respect to expenditures by such tribe or organization that are made for purposes specified in paragraph (b) of this clause and are permitted by other Federal law.

Reasonable compensation means, with respect to a regularly employed officer or employee of any person, compensation that is consistent with the normal compensation for such officer or employee for work that is not furnished to, not funded by, or not furnished in cooperation with the Federal Government.

Reasonable payment means, with respect to professional and other technical services, a payment in an amount that is consistent with the amount normally paid for such services in the private sector.

Recipient includes the Contractor and all subcontractors. This term excludes an Indian tribe, tribal organization, or any other Indian organization eligible to receive Federal contracts, grants, cooperative agreements, or loans from an agency, but only with respect to expenditures by such tribe or organization that are made for purposes specified in paragraph (b) of this clause and are permitted by other Federal law.

Regularly employed means, with respect to an officer or employee of a person requesting or receiving a Federal contract, an officer or employee who is employed by such person for at least 130 working days within 1 year immediately preceding the date of the submission that initiates agency consideration of such person for receipt of such contract. An officer or employee who is employed by such person for less than 130 working days within 1 year immediately preceding the date of the submission that

initiates agency consideration of such person shall be considered to be regularly employed as soon as he or she is employed by such person for 130 working days.

State means a State of the United States, the District of Columbia, or an outlying area of the United States, an agency or instrumentality of a State, and multi-State, regional, or interstate entity having governmental duties and powers.

(b) *Prohibition.* 31 U.S.C. 1352 prohibits a recipient of a Federal contract, grant, loan, or cooperative agreement from using appropriated funds to pay any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any covered Federal actions. In accordance with 31 U.S.C. 1352, the Contractor shall not use appropriated funds to pay any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the award of this contractor the extension, continuation, renewal, amendment, or modification of this contract.

(1) The term *appropriated funds* does not include profit or fee from a covered Federal action.

(2) To the extent the Contractor can demonstrate that the Contractor has sufficient monies, other than Federal appropriated funds, the Government will assume that these other monies were spent for any influencing activities that would be unallowable if paid for with Federal appropriated funds.

(c) *Exceptions.* The prohibition in paragraph (b) of this clause does not apply under the following conditions:

(1) *Agency and legislative liaison by Contractor employees*.

(i) Payment of reasonable compensation made to an officer or employee of the Contractor if the payment is for agency and legislative liaison activities not directly related to this contract. For purposes of this paragraph, providing any information specifically requested by an agency or Congress is permitted at any time.

(ii) Participating with an agency in discussions that are not related to a specific solicitation for any covered Federal action, but that concern-

(A) The qualities and characteristics (including individual demonstrations) of the person’s products or services, conditions or terms of sale, and service capabilities; or

(B) The application or adaptation of the person’s products or services for an agency’s use.

(iii) Providing prior to formal solicitation of any covered Federal action any information not specifically requested but necessary for an agency to make an informed decision about initiation of a covered Federal action;

(iv) Participating in technical discussions regarding the preparation of an unsolicited proposal prior to its official submission; and

(v) Making capability presentations prior to formal solicitation of any covered Federal action by persons seeking awards from an agency pursuant to the provisions of the Small Business Act, as amended by Pub. L. 95-507, and subsequent amendments.

(2) *Professional and technical services*.

(i) A payment of reasonable compensation made to an officer or employee of a person requesting or receiving a covered Federal action or an extension, continuation, renewal, amendment, or modification of a covered Federal action, if payment is for professional or technical services rendered directly in the preparation, submission, or negotiation of any bid, proposal, or application for that Federal action or for meeting requirements imposed by or pursuant to law as a condition for receiving that Federal action.

(ii) Any reasonable payment to a person, other than an officer or employee of a person requesting or receiving a covered Federal action or an extension, continuation, renewal, amendment, or modification of a covered Federal action if the payment is for professional or technical services rendered directly in the preparation, submission, or negotiation of any bid, proposal, or application for that Federal action or for meeting requirements imposed by or pursuant to law as a condition for receiving that Federal action. Persons other than officers or employees of a person requesting or receiving a covered Federal action include consultants and trade associations.

(iii) As used in paragraph (c)(2) of this clause, "professional and technical services" are limited to advice and analysis directly applying any professional or technical discipline (for examples, see FAR 3.803(a)(2)(iii)).

(iv) Requirements imposed by or pursuant to law as a condition for receiving a covered Federal award include those required by law or regulation and any other requirements in the actual award documents.

(3) Only those communications and services expressly authorized by paragraphs (c)(1) and (2) of this clause are permitted.

(d) *Disclosure*.

(1) If the Contractor did not submit OMB Standard Form LLL, Disclosure of Lobbying Activities, with its offer, but registrants under the Lobbying Disclosure Act of 1995 have subsequently made a lobbying contact on behalf of the Contractor with respect to this contract, the Contractor shall complete and submit OMB Standard Form LLL to provide the name of the lobbying registrants, including the individuals performing the services.

(2) If the Contractor did submit OMB Standard Form LLL disclosure pursuant to paragraph (d) of the provision at FAR 52.203-11, Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions, and a change occurs that affects Block 10 of the OMB Standard Form LLL (name and address of lobbying registrant or individuals performing services), the Contractor shall, at the end of the calendar quarter in which the change occurs, submit to the Contracting Officer within 30 days an updated disclosure using OMB Standard Form LLL.

(e) *Penalties*.

(1) Any person who makes an expenditure prohibited under paragraph (b) of this clause or who fails to file or amend the disclosure to be filed or amended by paragraph (d) of this clause shall be subject to civil penalties as provided for by 31 U.S.C. 1352. An imposition of a civil penalty does not prevent the Government from seeking any other remedy that may be applicable.

(2) Contractors may rely without liability on the representation made by their subcontractors in the certification and disclosure form.

(f) Cost allowability. Nothing in this clause makes allowable or reasonable any costs which would otherwise be unallowable or unreasonable. Conversely, costs made specifically unallowable by the requirements in this clause will not be made allowable under any other provision.

(g) *Subcontracts*.

(1) The Contractor shall obtain a declaration, including the certification and disclosure in paragraphs (c) and (d) of the provision at FAR 52.203-11, Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions, from each person requesting or receiving a subcontract under this contract that exceeds the threshold specified in FAR 3.808 on the date of subcontract award. The Contractor or subcontractor that awards the subcontract shall retain the declaration.

(2) A copy of each subcontractor disclosure form (but not certifications) shall be forwarded from tier to tier until received by the prime Contractor. The prime Contractor shall, at the end of the calendar quarter in which the disclosure form is submitted by the subcontractor, submit to the Contracting Officer within 30 days a copy of all disclosures. Each subcontractor certification shall be retained in the subcontract file of the awarding Contractor.

(3) The Contractor shall include the substance of this clause, including this paragraph (g), in any subcontract that exceeds the threshold specified in FAR 3.808 on the date of subcontract award.

(End of Clause)

C.4 RFO 52.217-7 OPTION FOR INCREASED QUANTITY—SEPARATELY PRICED LINE ITEM (MAR 1989)

The Government may require the delivery of the numbered line item, identified in the Schedule as an option item, in the quantity and at the price stated in the Schedule. The Contracting Officer may exercise the option by written notice to the Contractor within 24 months of award. Delivery of added items shall continue at the same rate that like items are called for under the contract, unless the parties otherwise agree.

(End of Clause)

C.5 RFO 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 30 days.

(End of Clause)

C.6 RFO 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 any time before contract expiration; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 10 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 66 months.

(End of Clause)

C.7 RFO 52.219-8 UTILIZATION OF SMALL BUSINESS CONCERNS (NOV 2025) (Deviation)

(a) *Definitions*. As used in this contract—

HUBZone small business concern means a small business concern that meets the requirements described in 13 CFR 126.200, certified by the Small Business Administration (SBA) and designated by SBA as a HUBZone small business concern in the Small Business Search (SBS) and the System for Award Management (SAM).

Service-disabled veteran-owned small business (SDVOSB) concern means an SDVOSB concern that meets the requirements described in 13 CFR 128.300, is certified by SBA, and is designated by SBA as an SDVOSB concern in SBS and SAM.

Small business concern means a concern, including its affiliates, that is independently owned and operated, not dominant in its field of operation and qualified as a small business under the criteria and size standards in 13 CFR part 121, including the size standard that corresponds to the NAICS code assigned to the contract or subcontract.

Small disadvantaged business (SDB) concern means a small business concern under the size standard applicable to the acquisition, that-

(1) Is at least 51 percent unconditionally and directly owned (as defined at 13 CFR 124.105) by-

(i) One or more socially disadvantaged (as defined at 13 CFR 124.103) and economically disadvantaged (as defined at 13 CFR 124.104) individuals who are citizens of the United States; and

(ii) Each individual claiming economic disadvantage has a net worth not exceeding the threshold at 13 CFR 124.104(c)(2) after taking into account the applicable exclusions set forth at 13 CFR 124.104(c)(2); and

(2) The management and daily business operations of which are controlled (as defined at 13.CFR 124.106) by individuals, who meet the criteria in paragraphs (1)(i) and (ii) of this definition.

Veteran-owned small business (VOSB) concern means a small business concern-

(1) Not less than 51 percent of which is owned and controlled by one or more veterans (as defined at 38 U.S.C.101(2)) or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more veterans; and
(2) The management and daily business operations of which are controlled by one or more veterans.

Women-owned small business (WOSB) concern means a small business concern-

(1) That is at least 51 percent owned by one or more women, or, in the case of any publicly owned business, at least 51 percent of the stock of which is owned by one or more women;
(2) Whose management and daily business operations are controlled by one or more women; and

(3) That is certified by SBA or an approved third- party certifier in accordance with 13 CFR 127.300 and is designated by SBA as a WOSB concern in SBS and SAM.

(b) It is the policy of the United States that small business concerns, VOSB concerns, SDVOSB concerns, HUBZone small business concerns, SDB concerns, and WOSB concerns shall have the maximum practicable opportunity to participate in performing contracts let by any Federal agency, including contracts and subcontracts for subsystems, assemblies, components, and related services for major systems. It is further the policy of the United States that its prime contractors establish procedures to ensure the timely payment of amounts due pursuant to the terms of their subcontracts with small business concerns, VOSB concerns, SDVOSB concerns, HUBZone small business concerns, SDB concerns, and WOSB concerns.

(c)
(1) A joint venture qualifies as a small business concern if—
(i) Each party to the joint venture qualifies as small under the size standard for the solicitation; or
(ii) The protégé is small under the size standard for the solicitation in a joint venture comprised of a mentor and protégé with an approved mentor-protégé agreement under a SBA mentor-protégé program. (See 13 CFR 125.9(d).)
(2) A joint venture qualifies as a HUBZone small business concern if it complies with the requirements in 13 CFR 126.616(a) through (c).

(d) The Contractor hereby agrees to carry out this policy in the awarding of subcontracts to the fullest extent consistent with efficient contract performance. The Contractor further agrees to cooperate in any studies or surveys as may be conducted by the Small Business Administration or the awarding agency of the as may be necessary to determine the extent of the Contractor's compliance with this clause.

(e)
(1) Unless the Contractor has reason to question the representation, it may accept a subcontractor's written representations of its size and socioeconomic status as a small business or SDB, if the subcontractor represents that the size and socioeconomic status representations with its offer are current, accurate, and complete as of the date of the offer for the subcontract.

(2) Unless the Contractor has reason to question the representation, it may accept a subcontractor's representations of its size and socioeconomic status as a small business or SDB in the System for Award Management (SAM) if the subcontractor—
(i) Is registered in SAM; and
(ii) Represents that the size and socioeconomic status representations made in SAM are current, accurate and complete as of the date of the offer for the subcontract.

(3) The Contractor may not require that the subcontractor register in SAM for the purposes of representing size or socioeconomic status in connection with a subcontract.

(4) A contractor acting in good faith is not liable for misrepresentations made by its subcontractors regarding the subcontractor's size or socioeconomic status.

(5) The Contractor shall confirm that a subcontractor representing itself as a HUBZone small business concern, VOSB, SDVOSB, or WOSB concern is certified by SBA by checking SAM or SBS at https://search.certifications.sba.gov/.

(End of clause)

C.8 RFO 52.219-14 LIMITATIONS ON SUBCONTRACTING (NOV 2025) (DEVIATION)

(a) This clause does not apply to the unrestricted portion of a partial set-aside.

(b) *Definition. Similarly situated entity*, as used in this clause, means a first-tier subcontractor, including an independent contractor, that—

(1) Has the same small business program status as that which qualified the prime contractor for the award (*e.g.*, for a small business set-aside contract, any small business concern, without regard to its socioeconomic status); and

(2) Is considered small for the size standard under the North American Industry Classification System (NAICS) code the prime contractor assigned to the subcontract.

(c) *Applicability.* This clause applies only to—

(1) Contracts that have been set aside for any of the small business concerns identified in 19.000(a)(3);

(2) Part or parts of a multiple-award contract that have been set aside for any of the small business concerns identified in 19.000(a)(3);

(3) Contracts that have been awarded on a sole-source basis in accordance with sections 19.105, 19.106, 19.107, and 19.108;

(4) Orders expected to exceed the simplified acquisition threshold and that are set aside for small business concerns under multiple-award contracts, as described in 8.4 and 16.5;

(5) Orders, regardless of dollar value, that are set aside in accordance with sections 19.105, 19.106, 19.107, and 19.108 under multiple-award contracts, as described in 8.4 and 16.5; and

(6) Contracts using the HUBZone price evaluation preference to award to a HUBZone small business concern unless the concern waived the evaluation preference.

(d) *Independent contractors.* An independent contractor shall be considered a subcontractor.

(e) By submission of an offer and execution of a contract, the Contractor agrees that in performance of a contract assigned a North American Industry Classification System (NAICS) code for—

(1) Services (except construction), it will not pay more than 50 percent of the amount paid by the Government for contract performance to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count towards the prime contractor's 50 percent subcontract amount that cannot be exceeded. When a contract includes both services and supplies, the 50 percent limitation shall apply only to the service portion of the contract;

(2) Supplies (other than procurement from a nonmanufacturer of such supplies), it will not pay more than 50 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count towards the prime contractor's 50 percent subcontract amount that cannot be exceeded. When a contract includes both supplies and services, the 50 percent limitation shall apply only to the supply portion of the contract;

(3) General construction, it will not pay more than 85 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count towards the prime contractor's 85 percent subcontract amount that cannot be exceeded; or

(4) Construction by special trade contractors, it will not pay more than 75 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count towards the prime contractor's 75 percent subcontract amount that cannot be exceeded.

(f) The Contractor shall comply with the limitations on subcontracting as follows:

(1) For contracts, in accordance with paragraphs (c)(1), (2), (3) and (6) of this clause—
[Contracting Officer check as appropriate.]

☒ By the end of the base term of the contract and then by the end of each subsequent option period; or

☐ By the end of the performance period for each order issued under the contract.

(2) For orders, in accordance with paragraphs (c)(4) and (5) of this clause, by the end of the performance period for the order.

(g) A joint venture agrees that, in the performance of the contract, the applicable percentage specified in paragraph (e) of this clause will be performed by the aggregate of the joint venture participants.

(1) In a joint venture comprised of a small business protégé and its mentor approved by the Small Business Administration, the small business protégé shall perform at least 40 percent of the work performed by the joint venture. Work performed

by the small business protégé in the joint venture must be more than administrative functions.

(2) In an 8(a) joint venture, the 8(a) participant(s) shall perform at least 40 percent of the work performed by the joint venture. Work performed by the 8(a) participants in the joint venture must be more than administrative functions.

(End of clause)

C.9 RFO 52.219-16 LIQUIDATED DAMAGES-SUBCONTRACTING PLAN (NOV 2025) (Deviation)

(a) The Government will measure performance by applying the percentage goals to the total actual subcontracting dollars, or, if a commercial plan is involved, to the pro rata share of actual subcontracting dollars attributable to Government contracts covered by the commercial plan. If, at contract completion or, in the case of a commercial plan, at the close of the fiscal year for which the plan is applicable, the Contractor has failed to meet its subcontracting goals and the Contracting Officer decides in accordance with paragraph (b) of this clause that the Contractor failed to make a good faith effort to comply with its subcontracting plan, established in accordance with the clause in this contract entitled “Small Business Subcontracting Plan,” the Contractor shall pay the Government liquidated damages in a stated amount. The amount of probable damages attributable to the Contractor's failure to comply shall equal the actual dollar amount by which the Contractor failed to achieve each subcontract goal.

(b) Before the Contracting Officer makes a final decision that the Contractor has failed to make a good faith effort to comply with the subcontracting plan, the Contracting Officer shall give the Contractor written notice specifying the failure and permitting the Contractor to demonstrate the good faith efforts it made and to discuss the matter. The Contracting Officer may take failure to respond to the notice as an admission that no valid explanation exists. If, after consideration of all the pertinent data, the Contracting Officer finds that the Contractor failed to make a good faith effort to comply with the subcontracting plan, the Contracting Officer will issue a final decision to that effect and require that the Contractor pay the Government liquidated damages as provided in paragraph (a) of this clause.

(c) With respect to commercial plans, the Contracting Officer who approved the plan will perform the functions of the Contracting Officer under this clause on behalf of all agencies with contracts covered by the commercial plan.

(d) The Contractor has the right of appeal, under the clause in this contract entitled, Disputes, from any final decision of the Contracting Officer.

(e) Liquidated damages shall be in addition to any other remedies that the Government may have.

(End of clause)

C.10 RFO 52.222-90 ADDRESSING DEI DISCRIMINATION BY FEDERAL CONTRACTORS (DEVIATION APR 2026)

(a)*Definitions*. As used in this clause—

Program participation means membership or participation in, or access or admission to: training, mentoring, or leadership development programs; educational opportunities; clubs; associations; or similar opportunities that are sponsored or established by the contractor or subcontractor.

Racially discriminatory diversity, equity, and inclusion (DEI) activities means disparate treatment based on race or ethnicity in the recruitment, employment (e.g., hiring, promotions), contracting (*e.g.*, vendor agreements), program participation, or allocation or deployment of an entity's resources.

(b) In connection with the performance of work under this contract, the Contractor agrees as follows:

(1) The Contractor will not engage in any racially discriminatory DEI activities;

(2) The Contractor will furnish all information and reports, including providing access to books, records, and accounts, as required by the Contracting Officer, for purposes of ascertaining compliance with this clause;

(3) In the event of the Contractor's or a subcontractor's noncompliance with this clause, this contract may be canceled, terminated, or suspended in whole or in part, and the Contractor or subcontractor may be declared ineligible for further Government contracts;

(4) The Contractor will report any subcontractor's known or reasonably knowable conduct that may violate this clause to the Contracting Officer and take any appropriate remedial actions directed by the Contracting Officer; and

(5) The Contractor will inform the Contracting Officer if a subcontractor sues the Contractor and the suit puts at issue, in any way, the validity of this clause.

(6) The Contractor recognizes that compliance with the requirements of this clause are material to the Government's payment decisions for purposes of 31 U.S.C. 3729(b)(4).

(c) The Contractor must include the substance of this clause, including this paragraph (c), in subcontracts at any tier, including those for commercial products and commercial services, except those where the place of delivery or performance is outside the United States.

(End of Clause)

C.11 RFO 52.240-91 SECURITY PROHIBITIONS AND EXCLUSIONS (NOV 2025) (DEVIATION)

(a) *Definitions*. As used in this clause—

American Security Drone Act-covered foreign entity means an entity included on a list that the Federal Acquisition Security Council (FASC) develops and maintains and publishes in the System for Award Management (SAM) at *https://www.sam.gov* (section 1822 of Pub. L. 118-31, 41 U.S.C. 3901 note prec.).

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered application means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.

Covered article, as defined in 41 U.S.C. 4713(k), means:

(1) Information technology, as defined in 40 U.S.C. 11101, including cloud computing services of all types;
(2) Telecommunications equipment or telecommunications service, as those terms are defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);
(3) The processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program (see 32 CFR part 2002); or
(4) Hardware, systems, devices, software, or services that include embedded or incidental information technology.

Covered foreign country means The People's Republic of China.

Covered telecommunications equipment or services means—

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);
(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or
(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means—

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;
(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled—
(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or
(ii) For reasons relating to regional stability or surreptitious listening;
(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);
(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);
(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or
(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

FASC-prohibited unmanned aircraft system means an unmanned aircraft system manufactured or assembled by an American Security Drone Act—covered foreign entity.

FASCSA order means any of the following orders issued under the Federal Acquisition Supply Chain Security Act (FASCSA) requiring removing covered articles from executive agency information systems or excluding one or more named sources or named covered articles from executive agency procurement actions, as described in 41 CFR 201-1.303(d) and (e):
(1) The Secretary of Homeland Security may issue FASCSA orders that apply to civilian agencies, to the extent not covered by paragraph (2) or (3) of this definition. This type of FASCSA order may be referred to as a Department of Homeland Security (DHS) FASCSA order.
(2) The Secretary of Defense may issue FASCSA orders that apply to the Department of Defense (DoD) and national security systems other than sensitive compartmented information systems. This type of FASCSA order may be referred to as a DoD FASCSA order.
(3) The Director of National Intelligence (DNI) may issue FASCSA orders that apply to the intelligence community and sensitive compartmented information systems, to the extent not covered by paragraph (2) of this definition. This type of FASCSA order may be referred to as a DNI FASCSA order.

Information technology, as defined in 40 U.S.C. 11101(6)—
(1) Means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is

used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use—
(i) Of that equipment; or
(ii) Of that equipment to a significant extent in the performance of a service or the furnishing of a product;
(2) Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but
(3) Does not include any equipment acquired by a Federal contractor incidental to a Federal contract.

Intelligence community, as defined by 50 U.S.C. 3003(4), means the following—
(1) The Office of the Director of National Intelligence;
(2) The Central Intelligence Agency;
(3) The National Security Agency;
(4) The Defense Intelligence Agency;
(5) The National Geospatial-Intelligence Agency;
(6) The National Reconnaissance Office;
(7) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs;
(8) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy;
(9) The Bureau of Intelligence and Research of the Department of State;
(10) The Office of Intelligence and Analysis of the Department of the Treasury;
(11) The Office of Intelligence and Analysis of the Department of Homeland Security; or
(12) Such other elements of any department or agency as may be designated by the President or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

Interconnection arrangement means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connecting a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Kaspersky Lab-covered article means any hardware, software, or service that—
(1) Is developed or provided by a Kaspersky Lab-covered entity;
(2) Includes any hardware, software, or service developed or provided in whole or in part by a Kaspersky Lab-covered entity; or
(3) Contains components using any hardware or software developed in whole or in part by a Kaspersky Lab-covered entity.

Kaspersky Lab-covered entity means—
(1) Kaspersky Lab;
(2) Any successor entity to Kaspersky Lab, including any change in name, e.g., "Kaspersky";

(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or
(4) Any entity of which Kaspersky Lab has a majority ownership.

National security system, as defined in 44 U.S.C. 3552, means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—
(1) The function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or
(2) Is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Sensitive compartmented information means classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence.

Sensitive compartmented information system means a national security system authorized to process or store sensitive compartmented information.

Source means a non-Federal supplier, or potential supplier, of products or services, at any tier.

Subsidiary means an entity in which more than 50 percent of the entity is owned directly by a parent corporation or through another subsidiary of a parent corporation.
Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

Unmanned aircraft means an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft (49 U.S.C. 44801(11)).

Unmanned aircraft system means an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system (49 U.S.C. 44801(12)).

(b) *Prohibitions on providing or using specific products or services in performance of contract*. Unless a waiver or exception applies, the Contractor is prohibited from

providing any products or services to the Government or using in the performance of the contract any of the following:
(1) A covered application on any information technology owned or managed by the Government, or on any information technology used or provided by the Contractor under this contract, including equipment provided by the Contractor's employees (section 102 of Division R of the Consolidated Appropriations Act, 2023 (Pub. L. 117-328));
(2) A Kaspersky Lab-covered article (Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91));
(3) Covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system (paragraphs (a)(1)(A) of section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232)). This does not prohibit contractors from providing—
(i) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or
(ii) Telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) Prohibition on unmanned aircraft systems manufactured or assembled by American Security Drone Act—covered foreign entities.
(1) Prohibition. The Contractor is prohibited from—
(i) Delivering any FASC-prohibited unmanned aircraft system, which includes unmanned aircraft (i.e., drones) and associated elements (sections 1823 and 1826 of American Security Drone Act of 2023, within the National Defense Authorization Act for Fiscal Year 2024, Pub. L. 118-31, Div. A, Title XVIII, Subtitle B, 41 U.S.C. 3901 note prec.);
(ii) On or after December 22, 2025, operating a FASC-prohibited unmanned aircraft system in the performance of the contract (section 1824 of Pub. L. 118-31); and
(iii) On or after December 22, 2025, using Federal funds to procure or operate a FASC-prohibited unmanned aircraft system (section 1825 of Pub. L. 118-31).
(2) *Procedures*. The Contractor shall search SAM for the FASC-maintained list of American Security Drone Act—covered foreign entities before proposing, or using in performance of the contract, any unmanned aircraft system. Also, the Contractor shall ensure any effort or expenditure associated with a FASC-prohibited unmanned aircraft system is consistent with a corresponding exemption, exception, or waiver determination expressly stated in the contract.
(3) *Exemptions, exceptions, and waivers*. The prohibitions in paragraph (c) of this clause do not apply where the agency has determined an exemption, exception, or waiver applies, and the contract indicates that such a determination has been made. See sections 1823 through 1825 and 1832 of Public Law 118-31 for statutory requirements pertaining to exemptions, exceptions, and waivers.

(d) *Prohibition on using or providing specific products or services or conducting certain transactions regardless of connection to contract*.
(1) *Certain telecommunications and video surveillance equipment, systems, or services*.

(i) Unless an applicable waiver has been issued by the Government, the Contractor cannot use any equipment, systems, or services that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system (paragraph (a)(1)(B) of section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232)).

(ii) This prohibition applies to using covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. This does not prohibit the contractor from using—

(A) A service that connects to the facilities of a third party, such as backhaul, roaming, or interconnection arrangements; or

(B) Telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(2) *Office of Foreign Assets Control Restrictions*.

(i) Except as authorized by the Office of Foreign Assets Control (OFAC) in the Department of the Treasury, the Contractor shall not acquire, for use in the performance of this contract, any supplies or services if any proclamation, Executive order, or statute administered by OFAC, or if OFAC's implementing regulations at 31 CFR chapter V, would prohibit such a transaction by a person subject to the jurisdiction of the United States.

(ii) Except as authorized by OFAC, most transactions involving Cuba, Iran, and Sudan are prohibited, as are most imports from Burma or North Korea, into the United States or its outlying areas.

(A) For lists of entities and individuals subject to economic sanctions, see OFAC's List of Specially Designated Nationals and Blocked Persons at *https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists*.

(B) For more information about these restrictions, as well as updates, see OFAC's regulations at 31 CFR chapter V and at *https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information*.

(C) To conduct electronic screens of potential parties to regulated transactions, see the consolidated screening list at *https://www.trade.gov/consolidated-screening-list*, which consolidates multiple export screening lists of the Departments of Commerce, State, and the Treasury.

(3) *Sudan prohibition*. The Contractor is prohibited from conducting any restricted business operations in Sudan in accordance with Accountability and Divestment Act of 2007 (Pub. L. 110-174).

(4) *Iran prohibitions*.

(i) Unless an exception applies according to paragraph (d)(4)(iii) or the Government grants a waiver, the contractor shall not engage in certain activities or transactions relating to Iran (section 6(b)(1)(A) of Iran Sanctions Act (50 U.S.C. 1701 note).

(ii) Unless an exception applies according to paragraph (d)(4)(iii) or the Government grants a waiver, contractor shall not export certain sensitive technology to Iran, as determined by the President, and has an active exclusion in SAM (22 U.S.C. 8515).

(iii) The prohibition in paragraphs (d)(4)(i) and (d)(4)(ii) do not apply if the acquisition is subject to trade agreements and the offeror certifies that all the offered products are designated country end products or designated country construction material (see part 25).

(iv) Unless an exception applies or the Government grants a waiver, contractors are prohibited from knowingly engaging in any significant transaction (i.e., over $15,000) with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked according to the International Emergency Economic Powers Act (section 6(b)(1)(B) of Iran Sanctions Act (50 U.S.C. 1701 note)).

(e) *Governmentwide exclusion and removal orders*.

(1) Unless the Government has issued an applicable waiver, contractors shall not provide or use as part of the performance of the contract any covered article, or any products or services produced or provided by a source, if the covered article or the source is prohibited by an applicable FASCSA order as follows:

(i) For solicitations and contracts awarded by a Department of Defense contracting office, DoD FASCSA orders apply.

(ii) For all other solicitations and contracts, DHS FASCSA orders apply.

(2) The Contractor shall search for the phrase "FASCSA order" in the System for Award Management (SAM) at *https://www.sam.gov* to locate applicable FASCSA orders.

(3) The Government may identify in the solicitation other FASCSA orders that are not in SAM, which are effective and apply to the solicitation and resulting contract.

(4) A FASCSA order issued after the date of solicitation applies to this contract only if added by an amendment to the solicitation or modification to the contract (see FAR 40.204-1(c)).

(f)*Reasonable inquiry*. The contractor shall conduct a reasonable inquiry to determine if there are any prohibited products or services. The inquiry will look at any information in the entity's possession but does not need to include an internal or third-party audit.

(g) *Removal of prohibited products and services*. For Federal Supply Schedules, Governmentwide acquisition contracts, multi-agency contracts or any other procurement instrument intended for use by multiple agencies, upon notification from the Contracting Officer, during the performance of the contract, the Contractor shall promptly make any necessary changes or modifications to remove any product or service produced or provided by a source that this clause prohibits.

(h) *General report*.

(1) If the Contractor identifies or is notified by any source, (including a subcontractor at any tier), that any product or service provided or used (or to be provided or used) during contract performance does not comply with any prohibition in this clause, then the Contractor shall report the following information, or as much information is known, in writing to the contracting office as identified in paragraph (h)(2) within 72 hours:

(i) Contract number and order number, if applicable;

(ii) The specific prohibition the product or service is not complying with;

(iii) A description of the products or services that the Contractor identifies or has reason to suspect is prohibited (include brand; model number, such as the original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);

(iv) The entity that produced the product or service (include entity name, unique entity identifier, Contractor and Government Entity (CAGE) code, facilities responsible for design, fabrication, assembly, packaging, and test of the product, and whether the entity was the OEM or a distributor (provide manufacturer codes and distributor codes used for the product));

(v) Description of the functionality of the product or service and how that functionality impacts the risk to the product or service;

(vi) An explanation of any factors relevant to determining if the product or service should be permitted by an applicable exception, exemption, or waiver (if the contractor would like the Government to consider a waiver, and asks for such a waiver);
(vii) Whether alternative products or services are available that would comply with the prohibition;
(viii) If the product or service is related to item maintenance, include the following information on the item being maintained:
(A) Brand;
(B) Model number, OEM number, manufacturer part number, or wholesaler number; and
(C) Item description, as applicable.
(ix) Any readily available information about mitigation actions implemented or recommended.
(2) If a report must be submitted to a contracting office, the Contractor shall submit the report as follows:
(i) If a Department of Defense contracting office, the Contractor shall report to the website at *https://dibnet.dod.mil*.
(ii) For all other contracting offices, the Contractor shall report to the Contracting Officer.
(iii) For indefinite delivery contracts, the Contractor shall report to both the contracting office for the indefinite delivery contract and the contracting office for any affected order.
(3) If the report provided does not contain any of the information required by paragraph (h)(1) of this clause, and the contractor later discovers new information that is required by paragraph (h)(1) of this clause, then the contractor shall submit a subsequent report within 72 hours of discovering the new information.
(4) The contractor shall also report the information in paragraph (h)(1) if the contractor wishes to ask for a waiver of the requirements of a new FASCSA order being applied through modification.
(i) *New FASCSA orders report*.
(1) During contract performance, the Contractor shall review SAM at least once every three months, or as advised by the Contracting Officer, to check for covered articles subject to FASCSA order(s), or for products or services produced by a source subject to FASCSA order(s) not currently identified under paragraph (e) of this clause.
(2) If the Contractor identifies a new FASCSA order(s) that could impact their supply chain, then the Contractor shall conduct a reasonable inquiry to identify whether a covered article or product or service produced or provided by a source subject to the FASCSA order(s) was provided to the Government or used during contract performance. The inquiry will look at any information in the entity's possession but does not need to include an internal or third-party audit.
(3) The Contractor shall submit a report to the contracting office identified in paragraph (h)(2) of this clause if the Contractor identifies, including through any notification by a subcontractor at any tier, that a covered article or product or service produced or provided by a source was provided to the Government or used during contract performance and is subject to a FASCSA order(s). For indefinite delivery contracts, the Contractor shall report to both the contracting office for the indefinite delivery contract and the contracting office for any affected order. The Contractor shall report the following information within 72 hours for each covered article or each product or service produced or provided by a source, where the covered article or source is subject to a FASCSA order:

(i) Contract number and order number, if applicable;
(ii) Name of the covered article or source subject to a FASCSA order;
(iii) The specific FASCSA order the product or service does not comply with;
(iv) The elements of (h)(1)(iii) through (ix) of this clause.
(j) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (j) but excluding subparagraphs (d)(1) and (i)(1), in all subcontracts and other contractual instruments, including subcontracts for acquiring commercial products or commercial services.

(End of clause)

C.12 VAAR 852.211-76 LIQUIDATED DAMAGES – REIMBURSEMENT FOR DATA BREACH COSTS (FEB 2023) ALTERNATE I (FEB 2023)

(a) *Definition*. As used in this clause, contract'' means any contract, agreement, order or other instrument and encompasses the definition set forth in FAR 2.101.

(b) *Non-disclosure requirements*. As a condition of performance under a contract, order, agreement, or other instrument that requires access to sensitive personal information as defined in VAAR 802.101, the following is expressly required—

(1) The Contractor, subcontractor, their employees or business associates shall not, directly or through an affiliate or employee of the Contractor, subcontractor, or business associate, disclose sensitive personal information to any other person unless the disclosure is lawful and is expressly permitted under the contract; and

(2) The Contractor, subcontractor, their employees or business associates shall immediately notify the Contracting Officer and the Contracting Officer's Representative (COR) of any security incident that occurs involving sensitive personal information.

(c) *Liquidated damages*. If the Contractor or any of its agents fails to protect VA sensitive personal information or otherwise engages in conduct which results in a data breach, the Contractor shall, in place of actual damages, pay to the Government liquidated damages of $37.50 per affected individual in order to cover costs related to the notification, data breach analysis and credit monitoring. In the event the Contractor provides payment of actual damages in an amount determined to be adequate by the Contracting Officer, the Contracting Officer may forgo collection of liquidated damages.

(d) *Purpose of liquidated damages*. Based on the results from VA's determination that there was a data breach caused by Contractor's or any of its agents' failure to protect or otherwise engaging in conduct to cause a data breach of VA sensitive personal information, and as directed by the Contracting Officer, the Contractor shall be responsible for paying to the VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of the following:

(1) Notification related costs.
(2) Credit monitoring reports.

(3) Data breach analysis and impact.
(4) Fraud alerts.
(5) Identity theft insurance.

(e) *Relationship to termination clause, if applicable*. If the Government terminates this contract in whole or in part under the Termination for cause paragraph, FAR 52.212–4(m), Contract Terms and Conditions—Commercial Products and Commercial Services, the Contractor is liable for damages accruing until the Government reasonably obtains delivery or performance of similar supplies or services. These damages are in addition to costs of repurchase as may be required under the Termination clause.

(End of Clause)

C.13 VAAR 852.204-72 PERSONNEL VETTING AND CREDENTIALING (DEVIATION) (MAR 2026)

(a) Definitions. As used in this clause –
VA Information system is the same as information system and means, pursuant to 38 U.S.C. 5727, a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information whether automated or manual.

VA sensitive information means all VA data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information and includes sensitive personal information. The term includes information where improper use or disclosure could adversely affect the ability of VA to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of Federal programs.

(b) *General*. Contractor personnel assigned to work for or on behalf of VA must undergo a background investigation commensurate with the risk and sensitivity level designation associated with the work to be performed at the level indicated in the contract. The Contractor and subcontractors shall comply with VA Directive/Handbook 0710, Personnel Security and Suitability Program, which can be accessed at: https://vaww.va.gov/vapubs/index.cfm.

(c) *Risk and Sensitivity Levels*. The following table identifies the risk and sensitivity levels that apply to any personnel providing services under this contract. *VA

Administrations, organizations and staff offices will use the OPM Position Designation Tool.

Positions/Tasks Designated as Non-Sensitive Positions – Tier 1/Low Risk
Positions/Tasks Designated as Non-Sensitive Positions – Tier 2/Mod Risk
Positions/Tasks Designated as Non-Sensitive Positions – Tier 4/High Risk

Security clearances are granted to individuals with a specific requirement for access to classified material (for example, Confidential, Secret and Top Secret). Contractor personnel that are required to obtain a security clearance will be subject to a Tier 3 or Tier 5 investigation. The following sensitivity designations have been assigned for the identified Tier 3 and Tier 5 required by this contract:
Tier 3:
Tier 5:

(d) *Fitness*. The results from a background investigation are used to determine if an individual's fitness is sufficient for that individual to perform work for or on behalf of VA in the position identified in this contract. Contractor fitness determinations are made in accordance with 5 CFR Part 731.202.

Fitness requirements for employment are separate and distinct from job qualifications. If a Contractor or subcontractor employee is found to be unsuitable or unfit to provide services under this contract, the Contractor shall immediately remove the employee from working on this contract and take those necessary steps that restrict the employee's logical access to VA data, information, VA sensitive information, or information technology or VA information systems containing such data or information.

The Contractor shall advise the employee that they are not permitted to access any VA controlled building or real property in relation to this contract. The removal of an unfit Contractor or subcontractor employee does not alleviate the Contractor from satisfying

the requirements of this contract. The Government will not reimburse the Contractor for any costs associated with the recruitment/replacement of an employee or subcontractor employee who is found to be unfit.

(e) *Identification Cards*. The Government will provide a Personal Identification Verification (PIV) card or other identification card, as necessary, to fit Contractor personnel who require physical access to VA facilities and/or logical access to VA data, information, VA sensitive information, or information technology or VA information systems containing such data or information. Contractor and subcontractor personnel shall prominently display their PIV/identification card on their persons while working at a VA facility and shall present their PIV/identification card for inspection upon request by a VA official. The Contractor must surrender the employee or subcontractor employee's PIV/identification card in accordance with the requirements set forth in Directive/Handbook 0735 when any of the following events occur:

1. When no longer needed for contract performance.
2. Upon completion of the Contractor/subcontractor employee's employment.
3. Upon contract completion or termination.

(f) *Lost/stolen*. Immediately upon detection, the Contractor shall report a lost or stolen PIV/identification card to the Government authorities as identified in Directive/Handbook 0735. Within 48 hours of reporting the lost/stolen PIV/identification card, the Contractor shall submit to the Program Manager an incident report that describes the relevant facts and circumstances regarding the loss/theft. If the loss/theft was reported by the Contractor to the local police, the Contractor shall further submit a copy of the final police report to the Program Manager within 48 hours of the report being made available by the local police department. The Government will not reimburse the Contractor for any costs that result from lost/stolen PIV/identification card(s).

(g) *Regular Reporting*. The Contractor shall submit a status report to PIV Sponsor within 5 working days after the end of each calendar quarter and as requested by the Government in order to initiate contract closeout procedures. The report must provide the status of each contractor/subcontractor employee who is required to have a PIV/identification card during the performance of the contract. The report shall identify the Contractor and the contract number, and list the following status for each contractor/subcontractor employee who holds a PIV/identification card under this contract:

1. Contractor/subcontractor employee name.
2. Name of VA facility where Contractor/subcontractor employee works, if applicable.
3. Date background check submitted for Contractor/subcontractor employee.
4. Date PIV/identification card issued to Contractor/subcontractor employee.
5. Contractor/subcontractor employee's PIV/identification card number, as applicable.
6. Date Contractor/subcontractor employee no longer has need for PIV/identification card.
7. Date Contractor notified VA that PIV/identification card is no longer required.
8. Date Contractor returned PIV/identification card was returned to VA.

(h) *Flow down of clause*. The Contractor shall include the substance of this clause in subcontracts, third-party agreements, and BAA's, in which subcontractors, third-party servicers/employees, and business associates will perform functions where they will have physical access to a VA facility or logical access to VA data, information, VA sensitive information, or information technology or VA information system containing such data or information.

(End of Clause)

C.14 VAAR 852.239-76 INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY (FEB 2023)

(a) All information and communication technology (ICT) (formerly referred to as electronic and information technology (EIT)) supplies, information, documentation and services support developed, acquired, maintained or delivered under this contract or order must comply with the ''Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards'' (see 36 CFR part 1194). Information about Section 508 is available at *http://www.section508.va.gov/*.

(b) The Section 508 accessibility standards applicable to this contract or order are identified in the specification, statement of work, or performance work statement. If it is determined by the Government that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(c) The Section 508 accessibility standards applicable to this contract are:

(d) In the event of a modification(s) to this contract or order, which adds new EIT supplies or services or revises the type of, or specifications for, supplies or services, the Contracting Officer may require that the Contractor submit a completed VA Section 508 Checklist and any other additional information necessary to assist the Government in determining that the ICT supplies or services conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(e) If this is an Indefinite-Delivery type contract, a Blanket Purchase Agreement or a Basic Ordering Agreement, the task/delivery order requests that include ICT supplies or services will define the specifications and accessibility standards for the order. In those cases, the Contractor may be required to provide a completed VA Section 508 Checklist and any other additional information necessary to assist the Government in determining that the ICT supplies or services conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the provided documentation, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(End of Clause)

C.15 MANDATORY WRITTEN DISCLOSURES

Mandatory written disclosures required by RFO clause 52.203-13 to the Department of Veterans Affairs, Office of Inspector General (OIG) must be made electronically through the VA OIG Hotline at https://www.vaoig.gov/hotline/online-forms and clicking on "RFO clause 52.203-13 Reporting." If you experience difficulty accessing the website, call the Hotline at 1-800-488-8244 for further instructions.

C.16 H CLAUSE ARTIFICIAL INTELLIGENCE IN VA CONTRACT

For purposes of this clause, AI is defined as set forth by VA and Section 238(g) of the National Defense Authorization Act for Fiscal Year 2019 to include:

1. Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
2. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
3. An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
4. A set of techniques, including machine learning (ML), that is designed to approximate a cognitive task.
5. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

The Contractor shall provide a list of all AI it will be proposing, creating, delivering, and/or using as part of contract performance, for VA approval. The list of AI shall be provided directly to the VA PM, COR, and CO at least annually but also at the following times: upon proposal submission, contract award, the COR's request, and upon the Contractor's proposed use of new AI tools not contemplated at the time of last reporting. AI shall not be used in performance of the contract without the written approval and authorization of the CO. The Contractor shall also report all AI intended for use in contract performance for VA's inclusion in the VA AI Use Case Inventory. The Contractor shall actively engage in AI discovery, assessment, and compliance activities undertaken by VA.

Once the Contractor has obtained CO authorization to use specific AI in contract performance, the Contractor shall provide the COR a signed Statement of Attestation prior to AI implementation. All AI for delivery and/or use in performance of the contract shall adhere to the *VA Trustworthy AI Framework*, available at https://department.va.gov/ai/trustworthy/. The Statement of Attestation shall include, but is not limited to, a description of all controls, processes, technologies, and mechanisms utilized to satisfy VA's six (6) AI Principles: Purposeful, Effective and Safe, Secure and Private, Fair and Equitable, Transparent and Explainable, and Accountable and

Monitored. The Statement of Attestation shall also certify that the Contractor owns or possesses all legally required rights, copyright, and licenses to use the specified AI. The Statement of Attestation shall clearly state that the use of the AI by VA personnel in performance of the contract:

1. Does not and will not infringe upon any intellectual property rights of any kind.
2. Does not violate any intellectual property rights of any kind.
3. Does not violate any other third-party rights of any kind.

The Statement of Attestation shall also affirm that there have not been any persisting or existing material errors, defects, failures, or interruptions in AI performance of its intended purpose. Additionally, the Statement of Attestation shall include the Contractor's endorsement that the AI has materially performed in accordance with its specifications and intended purpose. Lastly, the Statement of Attestation shall be updated and resubmitted, at a minimum, annually, prior to the exercise of any contract option periods. The Statement of Attestation shall be deemed separate from, and in addition to, the Contractor's reporting requirements relative to the use of AI. The Statement of Attestation is a material term of the contract; accordingly, failure to provide the Statement of Attestation, to include all requirements, may be deemed a breach of contract and thus, cause for termination.

Data Ownership and Use. VA data ("Data") shall include data collected, used, processed, stored, or generated as the result of the use of AI. VA data is and shall remain the sole and exclusive property of VA. Contractor is provided a limited, non-exclusive license to access and use Data solely for performing its obligations under the Contract. The Contractor shall: (a) keep and maintain VA data in strict confidence and as further described in this Contract and applicable law to avoid unauthorized access, use, disclosure, or loss; (b) not use, sell, rent, transfer, distribute, or otherwise disclose or make available VA Data for Contractor's own purposes or for the benefit of anyone other than VA without the CO's prior written consent; and (c) not store, use, and transmit VA Data outside of the United States. This applies to both identified and de-identified data.

The Contractor (or Subcontractor at any tier, including affiliates, third-party affiliates, and any other non-VA entities) shall not sell, monetize, release, share, reuse, transfer, or misuse any VA data, to include any models, training data, testing data, patterns, documentation, implementation artifacts, runtime artifacts, or any other digital artifacts, partially or as a whole, derived from AI or machine learning (ML) without the express written consent and approval from the CO.

The Contractor is prohibited from using non-public VA data, including Veteran data, and outputted results to train publicly or commercially available AI algorithms, fine-tune, or otherwise develop AI or ML models for reuse, transfer, or commercial purposes, without the express written authorization from the CO specifying VA data that may be used along with the acceptable scope of such usage. Contractor agrees that any AI models, weights, or derivative artifacts trained, or fine-tuned, on VA non-public data, if authorized by VA, may not be commercialized or used for the benefit of any third party without prior written approval by the CO and must be conducted within a VA authorized environment that has obtained an Authority to Operate

The Contractor shall indemnify VA and its officers, employees, and agents against liability, including costs, for actual or alleged direct or contributory infringement of, or inducement to infringe, any United States or foreign patent, trademark, or copyright, arising out of VA use of any AI products and/or services under the contract.

The Contractor shall maintain commercially reasonable insurance coverage for claims or losses pertaining to the AI products or services being used in performance of the contract.

The Contractor shall maintain commercially reasonable and industry standard conforming security safeguards and controls, including proper access controls for the AI. The Contractor agrees the VA Contracting Officer has the unilateral right to require deactivation of any AI for any reason and without notice.
Any development and/or creation of AI, including any AI derivatives, during performance of this contract, is subject to applicable Intellectual Property and data rights clauses under the Federal Acquisition Regulation (FAR) including, FAR 52.227-14. The VA retains the unlimited right to reuse, share, and/or redeploy AI code and AI models procured under this contract. License rights in any Commercial Computer Software shall be governed by this contract.
This clause applies to both existing and new uses of AI, both stand-alone AI and AI embedded within other systems or applications, AI developed both by VA or by third parties on behalf of agencies for the fulfilment of specific VA missions, including relevant data inputs used to train AI and outputs used in support of decision making, and VA procurement of AI applications.

This clause does not apply to AI embedded within common commercial products, such as word processors or map navigation systems. The Contractor shall inform the VA Contracting Officer in writing if it believes the AI it intends to use during contract performance is not covered by this clause. The burden to demonstrate the AI is a common commercial product shall rest solely with the Contractor.

Non-compliance with the terms above, or loss of sensitive VA medical records information resulting from AI use (whether accidental or intentional), may result in Contractor liability to VA for any and all rights and remedies provided by law, including but not limited to contract termination, liquidated damages, and referral to VA's Suspension and Debarment Committee.

The Contractor shall include the substance of this clause in all subcontracts, including Subcontractors at any tier, affiliates, third-party affiliates, and any other non-VA entities.

C17. BUSINESS ASSOCIATE AGREEMENT

(a) Incorporation. The Business Associate Agreement (BAA), set forth at Attachment 1 to this solicitation/contract, is hereby incorporated into and made a part of this contract by reference. The Contractor shall execute the BAA prior to performing any work involving the creation, receipt, maintenance, or transmission of Protected Health Information (PHI) on behalf of the Department of Veterans Affairs (VA), Veterans Health Administration (VHA).

(b) Applicability to Base and Option Periods. The BAA applies to the base period of performance and to all option periods exercised under this contract in accordance with Section C, clause 52.217-9, Option to Extend the Term of the Contract (or successor/equivalent clause). The Contracting Officer's exercise of any option period shall automatically extend the applicability of the BAA for the duration of that option period. No lapse in BAA coverage shall occur between the base period and any subsequently exercised option period, and between any two consecutive option periods, provided the Contractor continues to create, receive, maintain, or transmit PHI under this contract.

(c) No Re-Execution Required. Exercise of an option period under this contract shall not require re-execution of the BAA unless the Contracting Officer determines that a modification to the BAA is necessary. In the event of such a determination, the Contracting Officer shall issue a bilateral modification incorporating the revised BAA terms, and the Contractor shall execute the revised BAA prior to continued performance involving PHI.

(d) Survival. Consistent with Section 6 (Termination) of the BAA, the BAA remains in effect until the completion of the Contractor's duties under this contract or termination of this contract, whichever occurs first, and certain obligations of the Contractor (including but not limited to breach notification, safeguarding, and return or destruction of PHI) survive termination of the BAA and/or this contract as set forth in Section 6.E of the BAA.

(e) Conflict. In the event of a conflict between the terms of this clause and the BAA at Attachment 1, the terms of the BAA shall control with respect to HIPAA/HITECH compliance obligations; this clause governs solely the administrative applicability of the BAA across the base and option periods of this contract.

(f) Subcontractors. Where the Contractor engages subcontractors that will create, receive, maintain, or transmit PHI in connection with performance under any period of this contract, the Contractor shall ensure such subcontractors are bound by written agreements at least as restrictive as the BAA, consistent with Section 3.H of the BAA, for the full duration of the subcontractor's involvement, including any option periods.

SECTION D – CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS

*Attachment will be removed from any resulting award document.

D.1 LIST OF ATTACHMENTS

The following documents are attached to and incorporated into this solicitation/contract:

Attachment No.	Title	Purpose
Attachment 1	Business Associate Agreement (BAA)	Establishes contractor obligations regarding the use, disclosure, and safeguarding of Protected Health Information (PHI) in accordance with HIPAA
*Attachment 2	Past Performance Questionnaire (PPQ)	Collects past performance information from contractor-identified references for evaluation purposes

D.2 ATTACHMENT 1 – BUSINESS ASSOCIATE AGREEMENT

Attachment 1, Business Associate Agreement (BAA), is incorporated into this solicitation/contract in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and 45 CFR Parts 160 and 164 (the "HIPAA Rules").

The Contractor shall execute the BAA at Attachment 1 prior to award, or as directed by the Contracting Officer, if the Contractor will create, receive, maintain, or transmit Protected Health Information (PHI) on behalf of the Department of Veterans Affairs (VA) in the performance of this contract. The Contractor shall comply with all terms and conditions of the executed BAA throughout the period of performance, including any option periods exercised.

The Contractor shall ensure that any subcontractor that creates, receives, maintains, or transmits PHI on the Contractor's behalf agrees, in writing, to the same restrictions, conditions, and requirements that apply to the Contractor under the BAA, in accordance with 45 CFR 164.504(e)(2)(ii)(D).

Failure to execute or comply with the BAA at Attachment 1 may render the Contractor ineligible for award or may constitute grounds for termination in accordance with the terms of the contract.

D.3 ATTACHMENT 2 – PAST PERFORMANCE QUESTIONNAIRE

Attachment 2, Past Performance Questionnaire (PPQ), is provided for use by the Offeror in obtaining past performance information from references in support of the Offeror's proposal.

The Offeror is responsible for:

a. Distributing a copy of Attachment 2 to each reference identified in the Offeror's proposal for contracts/task orders cited as relevant past performance;
b. Requesting that each reference complete and submit the PPQ directly to the Government point of contact identified in Section E, at or before the proposal due date; and

c. Confirming with each reference that the completed questionnaire(s) were submitted in accordance with the instructions provided.

The Government reserves the right to use PPQs received, past performance information obtained through other sources such as CPARS and or interviews, or a combination thereof, in its evaluation of past performance under Section E. Offerors are cautioned that the Government is not obligated to request or wait for the submission of a PPQ from a reference and may proceed with evaluation based on information available at the time of evaluation. It is the Offeror's responsibility to ensure timely submission by its references; late or missing questionnaires may result in the Government being unable to consider that reference in the past performance evaluation.

SECTION E - SOLICITATION PROVISIONS

*Note that this section will be removed from the resulting award document.

ADDENDUM to FAR 52.212-1 INSTRUCTIONS TO OFFERORS—COMMERCIAL ITEMS

Provisions that are incorporated by reference (by Citation Number, Title, and Date), have 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 following provisions are incorporated into 52.212-1 as an addendum to this solicitation:

E.1 RFO 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 *Department of Veterans Affairs (VA) Acquisition Regulation (VAAR) (48 CFR Chapter 8)* provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of Provision)

E.2 RFO 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/far-overhaul/far-part-deviation-guide
https://www.va.gov/oal/library/vaar/

(End of Provision)

E.3 VAAR 852.252-70 SOLICITATION PROVISIONS OR CLAUSES INCORPORATED BY REFERENCE (JAN 2008)

The following provisions or clauses incorporated by reference in this solicitation must be completed by the offeror or prospective contractor and submitted with the quotation or offer. Copies of these provisions or clauses are available on the Internet at the Web sites provided in the provision at FAR 52.252-1, Solicitation Provisions Incorporated by

Reference, or the clause at FAR 52.252-2, Clauses Incorporated by Reference. Copies may also be obtained from the contracting officer.

RFO / VAAR Clause Number	Title	Date
52.203-11	Certification And Disclosure Regarding Payments to Influence Certain Federal Transactions	Sep 2024
52.203-18	Prohibition On Contracting with Entities That Require Certain Internal Confidentiality Agreements or Statements—Representation	Jan 2017
52.204-7	System For Award Management—Registration (Deviation)	Nov 2025
52.209-2	Prohibition On Contracting with Inverted Domestic Corporations—Representation (Deviation)	Nov 2025
52.212-1	Instructions To Offerors—Commercial Products and Commercial Services (Deviation)	Sep 2023
52.217-5	Evaluation Of Options (Deviation)	Nov 2025
52.219-4	Notice Of Price Evaluation Preference for HubZone Small Business Concerns (Deviation)	Nov 2025
52.229-11	Tax On Certain Foreign Procurements—Notice and Representation	Jun 2020
852.215-72	Notice Of Intent To Re-Solicit	Oct 2019
852.233-70	Protest Content/Alternative Dispute Resolution	Oct 2018
852.233-71	Alternate Protest Procedure	Oct 2018
852.239-71	Information System Security Plan and Accreditation	Feb 2023
852.239-75	Information And Communication Technology Accessibility Notice	Feb 2023

(End of Provision)

E.4 RFO 52.204-5 WOMEN-OWNED BUSINESS (OTHER THAN SMALL BUSINESS) (Oct 2014)

(a) Definition. “Women-owned business concern," as used in this provision, means a concern that is at least 51 percent owned by one or more women; or in the case of any publicly owned business, at least 51 percent of its stock is owned by one or more women; and whose management and daily business operations are controlled by one or more women.

(b) Representation. [Complete only if the offeror is a women-owned business concern and has not represented itself as a small business concern in paragraph (c)(1) of FAR 52.219-1, Small Business Program Representations, of this solicitation.] The offeror represents that it ☐ is a women-owned business concern.

(End of Provision)

E.5 RFO 52.209-5 CERTIFICATION REGARDING RESPONSIBILITY MATTERS (NOV 2025) (DEVIATION)

(a) (1) The Offeror certifies, to the best of its knowledge and belief, that—

(i) The Offeror and/or any of its Principals—

(A) Are ☐ are not ☐ presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency;

(B) Have □ have not □, within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State, or local) contract or subcontract; violation of Federal or State antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating Federal criminal tax laws, or receiving stolen property (if offeror checks "have", the offeror shall also see 52.209-7, if included in this solicitation);

(C) Are □ are not □ presently indicted for, or otherwise criminally or civilly charged by a governmental entity with, commission of any of the offenses enumerated in paragraph (a)(1)(i)(B) of this provision; and

(D) Have □, have not □, within a three-year period preceding this offer, been notified of any delinquent Federal taxes in an amount that exceeds the threshold at 9.104-5(a)(2) for which the liability remains unsatisfied. Federal taxes are considered delinquent if both of the following criteria apply:
(1) The tax liability is finally determined. The liability is finally determined if it has been assessed. A liability is not finally determined if a pending administrative or judicial challenge remains. In the case of a judicial challenge to the liability, the liability is not finally determined until all judicial appeal rights have been exhausted.
(2) The taxpayer is delinquent in making payment. A taxpayer is delinquent if the taxpayer has failed to pay the tax liability when full payment was due and required. A taxpayer is not delinquent in cases where enforced collection action is precluded.

(ii) The Offeror has □ has not □, within a 3-year period preceding this offer, had one or more contracts terminated for default by any Federal agency.
(2) "Principal," for the purposes of this certification, means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (*e.g.*, general manager; plant manager; head of a division or business segment; and similar positions).

(b) The Offeror shall provide immediate written notice to the Contracting Officer if, at any time prior to contract award, the Offeror learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

(c) A certification that any of the items in paragraph (a) of this provision exists will not necessarily result in withholding of an award under this solicitation. However, the

Government will consider the certification in connection with a determination of the Offeror's responsibility. Failure of the Offeror to furnish a certification or provide such additional information as requested by the Contracting Officer may render the Offeror non-responsible.

(d) This provision does not require establishment of a system of records in order to render, in good faith, the certification required by paragraph (a). The knowledge and information of an Offeror is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

(e) The certification in paragraph (a) of this provision is a material representation of fact upon which reliance was placed when making award. If the Government later determines that the Offeror knowingly rendered an erroneous certification, in addition to other remedies available to the Government, the Contracting Officer may terminate the contract resulting from this solicitation for default.

(End of Provision)

E.6 RFO 52.209-7 INFORMATION REGARDING RESPONSIBILITY MATTERS (OCT 2018)

(a) *Definitions.* As used in this provision—
"Administrative proceeding" means a non-judicial process that is adjudicatory in nature in order to make a determination of fault or liability (e.g., Securities and Exchange Commission Administrative Proceedings, Civilian Board of Contract Appeals Proceedings, and Armed Services Board of Contract Appeals Proceedings). This includes administrative proceedings at the Federal and State level but only in connection with performance of a Federal contract or grant. It does not include agency actions such as contract audits, site visits, corrective plans, or inspection of deliverables.
"Federal contracts and grants with total value greater than $10,000,000" means—
(1) The total value of all current, active contracts and grants, including all priced options; and
(2) The total value of all current, active orders including all priced options under indefinite-delivery, indefinite-quantity, 8(a), or requirements contracts (including task and delivery and multiple-award Schedules).
"Principal" means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (e.g., general manager; plant manager; head of a division or business segment; and similar positions).

(b) The offeror [ ] has [ ] does not have current active Federal contracts and grants with total value greater than $10,000,000.

(c) If the offeror checked "has" in paragraph (b) of this provision, the offeror represents, by submission of this offer, that the information it has entered in the Federal Awardee Performance and Integrity Information System (FAPIIS) is current, accurate, and complete as of the date of submission of this offer with regard to the following information:
(1) Whether the offeror, and/or any of its principals, has or has not, within the last five years, in connection with the award to or performance by the offeror of a Federal contract or grant, been the subject of a proceeding, at the Federal or State level that resulted in any of the following dispositions:

(i) In a criminal proceeding, a conviction.
(ii) In a civil proceeding, a finding of fault and liability that results in the payment of a monetary fine, penalty, reimbursement, restitution, or damages of $5,000 or more.
(iii) In an administrative proceeding, a finding of fault and liability that results in—
(A) The payment of a monetary fine or penalty of $5,000 or more; or
(B) The payment of a reimbursement, restitution, or damages in excess of $100,000.
(iv) In a criminal, civil, or administrative proceeding, a disposition of the matter by consent or compromise with an acknowledgment of fault by the Contractor if the proceeding could have led to any of the outcomes specified in paragraphs (c)(1)(i), (c)(1)(ii), or (c)(1)(iii) of this provision.
(2) If the offeror has been involved in the last five years in any of the occurrences listed in (c)(1) of this provision, whether the offeror has provided the requested information with regard to each occurrence.

(d) The offeror shall post the information in paragraphs (c)(1)(i) through (c)(1)(iv) of this provision in FAPIIS as required through maintaining an active registration in the System for Award Management, which can be accessed via *https://www.sam.gov* (see 52.204-7).

(End of Provision)

E.7 RFO 52.209-11 REPRESENTATION BY CORPORATIONS REGARDING DELINQUENT TAX LIABILITY OR A FELONY CONVICTION UNDER ANY FEDERAL LAW (NOV 2025) DEVIATION

The Government will not enter into a contract with any corporation that—

(1) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless an agency has considered suspension or debarment of the corporation and made a determination that suspension or debarment is not necessary to protect the interests of the Government; or

(2) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.

(b) The Offeror represents that–

(1) It is☐ is not ☐ a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability; and

(2) It is ☐ is not ☐ a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.

(End of Provision)

E.8 RFO 52.216-1 TYPE OF CONTRACT (NOV 2025) (DEVIATION)

The Government contemplates award of a Firm-Fixed-Price contract resulting from this solicitation.

(End of Provision)

E.9 RFO 52.233-2 SERVICE OF PROTEST (NOV 2025) (DEVIATION)

(a) Protests, (as defined in FAR 33.102), that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), must be served on the Contracting Officer identified in the solicitation by obtaining written and dated acknowledgment of receipt from them.

(b) The copy of any protest must be received in the office designated above within one day of filing a protest with the GAO.

(End of Provision)

E.10 RFO 52.227-15 REPRESENTATION OF LIMITED RIGHTS DATA AND RESTRICTED COMPUTER SOFTWARE DEC 2007

(a) This solicitation sets forth the Government's known delivery requirements for data (as defined in the clause at 52.227-14, Rights in Data—General). Any resulting contract may also provide the Government the option to order additional data under the Additional Data Requirements clause at 52.227-16, if included in the contract. Any data delivered under the resulting contract will be subject to the Rights in Data—General clause at 52.227-14 included in this contract. Under the latter clause, a Contractor may withhold from delivery data that qualify as limited rights data or restricted computer software, and deliver form, fit, and function data instead. The latter clause also may be used with its Alternates II and/or III to obtain delivery of limited rights data or restricted computer software, marked with limited rights or restricted rights notices, as appropriate. In addition, use of Alternate V with this latter clause provides the Government the right to inspect such data at the Contractor's facility.

(b) By completing the remainder of this paragraph, the offeror represents that it has reviewed the requirements for the delivery of technical data or computer software and states [offeror check appropriate block]

[ ] None of the data proposed for fulfilling the data delivery requirements qualifies as limited rights data or restricted computer software; or

[ ] Data proposed for fulfilling the data delivery requirements qualify as limited rights data or restricted computer software and are identified as follows:

_____

_____

_____

(c) Any identification of limited rights data or restricted computer software in the offeror's response is not determinative of the status of the data should a contract be awarded to the offeror.

(End of Provision)

E.11 RFO 52.240-90 SECURITY PROHIBITIONS AND EXCLUSIONS REPRESENTATIONS AND CERTIFICATIONS (NOV 2025) (DEVIATION)

(a) *Definitions.* As used in this provision—

Backhaul, covered article, covered telecommunications equipment or services, critical technology, FASCSA order, Intelligence community, interconnection arrangements, national security system, roaming, sensitive compartmented information, sensitive compartmented information system, source, and substantial or essential component have the meanings provided in the clause 52.240-91, Security Prohibitions and Exclusions.

Business operations means engaging in commerce in any form, including by acquiring, developing, maintaining, owning, selling, possessing, leasing, or operating equipment, facilities, personnel, products, services, personal property, real property, or any other apparatus of business or commerce.

Marginalized populations of Sudan means—
(1) Adversely affected groups in regions authorized to receive assistance under section 8(c) of the Darfur Peace and Accountability Act (Pub. L. 109-344) (50 U.S.C. 1701 note); and
(2) Marginalized areas in Northern Sudan described in section 4(9) of such Act.

Restricted business operations means business operations in Sudan that include power production activities, mineral extraction activities, oil-related activities, or the production of military equipment, as those terms are defined in the Sudan Accountability and Divestment Act of 2007 (Pub. L. 110-174). Restricted business operations do not include business operations that the person (as that term is defined in Section 2 of the Sudan Accountability and Divestment Act of 2007) conducting the business can demonstrate—
(1) Are conducted under contract directly and exclusively with the regional government of southern Sudan;
(2) Are conducted under specific authorization from the Office of Foreign Assets Control in the Department of the Treasury, or are expressly exempted under Federal law from the requirement to be conducted under such authorization;
(3) Consist of providing goods or services to marginalized populations of Sudan;
(4) Consist of providing goods or services to an internationally recognized peacekeeping force or humanitarian organization;
(5) Consist of providing goods or services that are used only to promote health or education; or
(6) Have been voluntarily suspended.

Sensitive technology—
(1) Means hardware, software, telecommunications equipment, or any other technology that is to be used specifically—

(i) To restrict the free flow of unbiased information in Iran; or
(ii) To disrupt, monitor, or otherwise restrict speech of the people of Iran; and
(2) Does not include information or informational materials the export of which the President does not have the authority to regulate or prohibit pursuant to section 203(b)(3) of the International Emergency Economic Powers Act (50 U.S.C. 1702(b)(3)).

(b) *Procedures*.
(1) *Covered telecommunications and video surveillance*. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) at *https://www.sam.gov* for entities excluded from receiving federal awards for "covered telecommunications equipment or services."

(2) *FASCSA Orders*.
(i) The Offeror shall search in SAM for the phrase "FASCSA order" for any covered article, or any products or services produced or provided by a source, if there is an applicable FASCSA order described in paragraph (e) of FAR 52.240-91, Security Prohibitions and Exclusions.
(ii) The Offeror shall review the solicitation for any FASCSA orders that are not in SAM but are effective and apply to the solicitation and resultant contract (see FAR 40.204-1(c)(2)).
(iii) FASCSA orders issued after the date of solicitation do not apply unless added by an amendment to the solicitation.

(c) *Covered telecommunications equipment or services representations*. By submission of its offer, the Offeror represents that, after conducting a reasonable inquiry (that looks at any information in the Offeror's possession but does not need to include an internal or third-party audit)—
(1) It will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation, except as waived by the solicitation, or as disclosed in paragraph (g); and
(2) It does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services, except as waived by the solicitation, or as disclosed in paragraph (g).

(d) *FASCSA Representation*. By submission of this offer, the offeror represents that it has conducted a reasonable inquiry, and that the offeror does not propose to provide or use in response to this solicitation any covered article, or any products or services produced or provided by a source, if the covered article or the source is prohibited by an applicable FASCSA order in effect on the date the solicitation was issued, except as waived by the solicitation, or as disclosed in paragraph (g). A reasonable inquiry will look at any information in the offeror's possession but does not need to include an internal or third-party audit.

(e) *Sudan certification*. By submission of its offer, the offeror certifies, after conducting a reasonable inquiry (that looks at any information in the offeror's possession but does not need to include an internal or third-party audit), that the offeror does not conduct any restricted business operations in Sudan.

(f) *Iran Representation and Certifications*.
(1) Except as provided in paragraph (f)(2) of this provision or if a waiver has been granted in accordance with FAR 40.203-3, the offeror, after conducting a reasonable inquiry (that looks at any information in the offeror's possession but does not need to include an internal or third-party audit), by submission of its offer—
(i) Represents, to the best of its knowledge and belief, that the offeror does not export any sensitive technology to the government of Iran or any entities or individuals owned or controlled by, or acting on behalf or at the direction of, the government of Iran;
(ii) Certifies that the offeror, or any person (as defined at section 15 of the Iran Sanctions Act of 1996, Pub. L. 104-172, 50 U.S.C. 1701 note) owned or controlled by the offeror, does not engage in any activities for which sanctions may be imposed under section 5 of the Act. These sanctioned activities are in the areas of development of the petroleum resources of Iran, production of refined petroleum products in Iran, sale and provision of refined petroleum products to Iran, and contributing to Iran's ability to acquire or develop certain weapons or technologies; and
(iii) Certifies that the offeror, and any person owned or controlled by the offeror, does not knowingly engage in any transaction that exceeds $15,000 with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (see OFAC's Specially Designated Nationals and Blocked Persons List at *https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx*)

(2) Exception for trade agreements. The representation and certification requirements of paragraph (f)(1) of this provision do not apply if—
(i) This solicitation includes a trade agreements notice or certification (e.g., 52.225-6, Trade Agreements Certificate); and
(ii) The offeror has certified that all the offered products to be supplied are designated country end products or designated country construction material.
(iii) The offeror shall email questions concerning sensitive technology to the Department of State at *CISADA106@state.gov*.

(g) *Disclosure*.
(1) If the Offeror is not able to represent compliance with the prohibitions in paragraphs (c) or (d), then the Offeror shall disclose within 72 hours to the contracting office identified in paragraph (g)(2) the following information for each product or service not compliant:
(i) Contract number and order number, if applicable;
(ii) Identification of whether this disclosure relates to paragraph (c) on covered telecommunication equipment or services, or to paragraph (d) on FASCSA orders;
(iii) A description of the products or services that the Contractor identifies or has reason to suspect is prohibited (include brand; model number, such as the original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);
(iv) The entity that produced the product or service (include entity name, unique entity identifier, Contractor and Government Entity (CAGE) code, facilities responsible for design, fabrication, assembly, packaging, and test of the product, and whether the entity was the OEM or a distributor (provide manufacturer codes and distributor codes used for the product));

(v) Description of the functionality of the product or service and how that functionality impacts the risk to the product or service;
(vi) An explanation of any factors relevant to determining if the product or service should be permitted by an applicable exception, exemption, or waiver (if the offeror would like the Government to consider a waiver);
(vii) Whether alternative products or services are available that would be compliant with the prohibition;
(viii) If the product or service is related to item maintenance, include the following information on the item being maintained:
(A) Brand;
(B) Model number, OEM number, manufacturer part number, or wholesaler number; and
(C) Item description, as applicable.
(ix) Any readily available information about mitigation actions undertaken or recommended.

(2) If a disclosure is required to be submitted to a contracting office, the offeror shall submit the disclosure as follows:
(i) If a Department of Defense contracting office, the offeror shall submit the disclosure to the website at *https://dibnet.dod.mil*.
(ii) For all other contracting offices, the Offeror shall submit the disclosure to the Contracting Officer.

(3) If the disclosure provided does not contain any of the information required by paragraph (1), and the Offeror later discovers new information that is required by paragraph (1), then the Offeror shall submit a subsequent disclosure within 72 hours of discovering the new information.

(h) *Executive agency review of disclosures*. The Contracting Officer will review disclosures provided in paragraph (g) to determine if any applicable waiver may be sought. The Contracting Officer may choose not to pursue a waiver and may instead make an award to an Offeror that does not require a waiver.

(End of Provision)

E.12 VAAR 852.215-72 NOTICE OF INTENT TO RE-SOLICIT (OCT 2019)

This solicitation provides offerors fewer than 30 days to submit proposals. In the event that only one offer is received in response to this solicitation, the Contracting Officer may cancel the solicitation and re-solicit for an additional period of at least 30 days in accordance with 815.370-2.

(End of Provision)

E.13 NEW SOLICITATION NOTICE

System updates may lag policy updates. The System for Award Management (SAM) may continue to require entities to complete representations based on provisions that are not included in agency solicitations. Contracting officers will not consider these representations when making award decisions or enforce requirements. Entities are not

required to, nor are they able to, update their entity registration to remove these representations in SAM.

E.14 EVALUATION

A. BASIS OF AWARD

Any award made will be based on the best overall (i.e., best value) proposal that is determined to be the most beneficial to the Government, with appropriate consideration given to the following evaluation factors: Technical, Past Performance, Veterans Involvement, and Price. The Technical Factor shall be comprised of a written Technical Approach, which is significantly more important than the Past Performance, which is slightly more important than the Veterans Involvement Factor. The non-Price Factors when combined are significantly more important than the Price Factor. To receive consideration for award, a rating of no less than “Acceptable” for the Technical Factor. Offerors are cautioned that any resulting award may not necessarily be made to the lowest Price offered or the most highly rated technical proposal. The Government intends to award one contract.

B. FACTORS TO BE EVALUATED

1. TECHNICAL
2. PAST PERFORMANCE
3. VETERANS INVOLVEMENT
4. PRICE

C. EVALUATION APPROACH

All proposals shall be subject to evaluation by a team of Government personnel. In accordance with RFO 15 and VAAR Subpart 815, the Government may establish a competitive range comprised of the most highly rated proposals, as determined by evaluation under the factors set forth herein. If the Contracting Officer determines that the number of most highly rated proposals exceeds the number at which meaningful and manageable comparisons can be effectively conducted, the competitive range may be limited to the greatest number of proposals that will sustain efficient, substantive discussions. Evaluation shall include consideration of SDVOSB/VOSB related factors in accordance with VAAR 815.304 70, including preference for offers received from VOSBs and additional preference for offers received from SDVOSBs. Only Offerors included in the competitive range will be invited to participate in negotiations. The Government reserves the right to award without negotiations; therefore, Offerors are urged to submit proposals that reflect their best terms from the outset. Offerors who fail to meet the minimum requirements of the solicitation will be rated Unacceptable and thus, ineligible for award.

1. TECHNICAL FACTOR: WRITTEN TECHNICAL APPROACH

The proposal will be evaluated strictly in accordance with its written content. Proposals which merely restate the requirement or state that the requirement will be met, without

providing supporting rationale, are not sufficient. The evaluation process will consider the following:

a. Understanding of the Problem - The proposal will be evaluated to determine the extent to which it demonstrates a clear understanding of all features involved in solving the problems and meeting and/or exceeding the requirements presented in the solicitation and the extent to which uncertainties are identified and resolutions proposed.

b. Feasibility of Approach - The proposal will be evaluated to determine the extent to which the proposed approach is workable and the end results achievable. The proposal will be evaluated to determine the level of confidence provided the Government with respect to the Offeror's methods and approach in successfully meeting and/or exceeding the requirements in a timely manner.

2. PAST PERFORMANCE EVALUATION APPROACH

The Past Performance evaluation will assess the relative risks associated with an Offeror's likelihood of success in fulfilling the solicitation's requirements as indicated by that Offeror's record of past performance. In this context, “Offeror” refers to the proposed prime contractor and all proposed major subcontractor(s). A major subcontractor is defined as one who will be providing COTS software and/or whose subcontract is for more than 30% of the proposed total price. In either case, the prime contractor and proposed major subcontractor(s) will be assessed individually and the results will then be assessed in their totality to derive the Offeror’s Past Performance rating.

The Government will conduct a performance risk assessment based on the quality of the Offeror’s recent and relevant past performance, as well as that of its major subcontractors, as it relates to the probability of successful accomplishment of the required effort. Offerors are cautioned that the Government will review past performance data available at any point during the three years immediately prior to the proposal submission date that is over a $2M and are relevant in the Contract Performance Assessment Reporting System (CPARS). Areas of relevance include integration, clinical workflow solution, data migration, interoperability, training, implementation, sustainment, and program management and execution of large-scale, multi-facility Mammography Tracking and Reporting system deployments within federal or complex healthcare environments. The Government reserves the right to obtain past performance information from any available source and may contact customers other than those identified by the Offeror when evaluating past performance. Since the Government may not necessarily interview all of the sources provided by the Offerors, it is incumbent upon the Offerors to explain the relevance of the data provided. Offerors are reminded that the burden of proving low performance risk rests with the Offerors.

The Government will review aspects of cost, schedule, and performance. Areas to be evaluated may include, but are not limited to, quality of product or service, timeliness of performance or adherence to delivery schedules, and/or effectiveness in program management (to include use and control of subcontractors).

In the case of an Offeror without a record of relevant past performance or for whom information on past performance is not available, the Offeror may not be evaluated favorably or unfavorably on Past Performance.

3. VETERANS INVOLVEMENT EVALUATION APPROACH

In accordance with Veterans Affairs Acquisition Regulation (VAAR) 852.215-70 (DEVIATION), Service-Disabled Veteran-Owned and Veteran-Owned Small Business (VOSB) Evaluation Factors, the Government will assign evaluation credit for an Offeror (prime contractor) which is a Service-Disabled Veteran-Owned Small Business (SDVOSB) or a VOSB. To receive credit, an offeror must be registered and verified in Small Business Administration (SBA) Small Business Certification Program, listed on the SBA Veteran Small Business Certification (VetCert) website at https://veterans.certify.sba.gov/ at time of proposal submission and at time of award, must meet federal small business size standards for the North American Industry Classification System (NAICS) code assigned to this solicitation at time of both proposal submission and at time of award.

Non-SDVOSB/VOSB Offerors proposing to use SDVOSBs or VOSBs as subcontractors will receive some consideration under this evaluation Factor. Offerors must state in their proposals the names of the SDVOSBs and VOSBs with whom they intend to subcontract and provide a brief description of the proposed subcontracts and the approximate dollar values of the proposed subcontracts. In addition, the proposed subcontractors must be registered and verified in the SBA Small Business Search database (https://search.certifications.sba.gov) and must meet federal small business size standards for the NAICS code assigned to this solicitation at time of both proposal submission and at time of award.

4. PRICE EVALUATION APPROACH

For Offerors from the Historically Underutilized Business Zone business concerns that have not waived the evaluation preference, a price evaluation preference will be applied in accordance with RFO 52.219-4.

The total overall evaluated price will be the sum of the total evaluated FFP line items, including all options and optional tasks. The total evaluated price for each line item will be calculated by multiplying the quantity/unit (e.g., 3 EA) by the proposed unit price. The Government will verify the Offeror’s calculation of the total overall evaluated price. The Government will adjust the Offeror’s proposed total overall evaluated price if mathematical errors are identified. All prices shall be rounded to the nearest cent. The Government reserves the right to correct any rounding errors identified in the Offeror’s offer/proposal. The total evaluated price shall be based on the information provided in Section B.4, Price Schedule.

Unbalanced Pricing - The Government may evaluate whether the Offeror has submitted unbalanced pricing. An unbalanced price is one where the price of one or more contract line items is significantly overstated or understated and which will result in the Government paying an unreasonably high price for contract performance or otherwise

present an unacceptable level of risk to the Government. If the Contracting Officer determines that the risk is unacceptable, then the offer can be rejected.

E.15 INSTRUCTIONS TO OFFEROR

1. PROPOSAL SUBMISSION INSTRUCTIONS

The Offeror's proposal shall be submitted electronically by the date and time indicated in the solicitation to Terricia Lloyd, Terricia.Lloyd@va.gov, and Brett Schwerin, Brett.Schwerin@va.gov, in the files set forth below by the date and time indicated in the solicitation. The Offeror's proposal shall consist of five Volumes. The Volumes are Volume One –Technical Factor, Volume Two - Past Performance, Volume Three – Past Performance, Volume Four – Price and Volume Five - Solicitation, Offer and Award Documents and Certifications/Representations.
The use of hyperlinks or embedded attachments in proposals is prohibited. Accordingly, any hyperlinks or embedded attachments included with a proposal will neither be accessed nor viewed by the Government and thus, not evaluated as part of the Offeror's proposal submission. Total submitted file size shall not exceed 5MB.

NOTE: Due to file size limitations, not all emails may be received, please request a receipt response to ensure files have been delivered; multiple emails may be required due to size limitations (5MB per email). If more than one email must be submitted, please number emails as appropriate, for example, "1 of total emails to be received (e.g., 1 of 3, 2 of 3 etc.). Proposals submitted by any other method will not be considered.

WARNING: Please do not wait until the last minute to submit your proposals! Late proposals will not be accepted for evaluation. To avoid submission of late proposals, we recommend the transmission of your proposal file 24 hours prior to the required proposal due date and time. Please be advised that timeliness is determined by the date and time an Offeror's proposal is received by the Government not when an Offeror attempted transmission. Offerors are encouraged to review and ensure that sufficient bandwidth is available on their end of the transmission.

Any concerns or questions regarding the submission of quotes shall be addressed by email to Terricia Lloyd, Terricia.Lloyd@va.gov, and Brett Schwerin, Brett.Schwerin@va.gov.

2. PROPOSAL FILES

Offeror's responses shall be submitted in accordance with the following instructions:

a. Format. The submission shall be clearly indexed and logically assembled. Each volume shall be clearly identified and shall begin at the top of a page. All pages of each volume shall be appropriately numbered and identified by the complete company name, date and solicitation number in the header and/or footer. Proposal page limitations are applicable to this procurement. The Table below indicates the maximum page count (when applicable) for each volume of the Offeror's proposal.

All files will be submitted as either a Microsoft Word 2010 (.doc) or later version, Microsoft Excel (.XLS) file or an Acrobat (PDF) file or compatible as indicated in the table. Page size shall be no greater than 8 1/2" x 11" with printing on one side, only. The top, bottom, left and right margins shall be a minimum of one inch (1”) each. Font size shall be no smaller than 12-point. Arial or Times New Roman fonts are required. Characters shall be set at no less than normal spacing and 100% scale. Tables and illustrations may use a reduced font size not less than 8-point and may be landscape. Line spacing shall be set at no less than single space. Each paragraph shall be separated by at least one blank line. Page numbers, company logos, headers and footers may be within the page margins ONLY and are not bound by the 12-point font requirement. Footnotes to text shall not be used. All proprietary information must be clearly and properly marked. If the Offeror submits annexes, documentation, attachments or the like, not specifically required by this solicitation, such will count against the Offeror’s page limitations unless otherwise indicated in the specific volume instructions below. Pages in violation of these instructions, either by exceeding the margin, font, printing, or spacing restrictions or by exceeding the total page limit for a particular volume, will not be evaluated. Pages not evaluated due to violation of the margin, font or spacing restrictions will not count against the page limitations. The page count will be determined by counting the pages in the order they come up in the print layout view.

b. File Packaging. All of the proposal files may be compressed (zipped) into one file entitled “proposal.zip” using WinZip version 6.2 or later version or the proposal files may be submitted individually.

c. Content Requirements. All information shall be confined to the appropriate file.

The Offeror shall confine submissions to essential matters, sufficient to define the proposal and provide an adequate basis for evaluation. Offerors are responsible for including sufficient details, in a concise manner, to permit a complete and accurate evaluation of each proposal. The titles and page limits requirements for each file are shown in the Table below:

Volume Number	Factor	File Name	Page Limitations
Volume I	Technical	Tech.pdf	25 Pages
Volume II	Past Performance	Past Perf.pdf	None
Volume III	Veterans Involvement	VetsI.pdf	None
Volume IV	Price	Price Exhibit.docx	None
Volume V	Solicitation, Offer & Award Documents, Certifications & Representations	OfrRep.pdf	None

A Cover Page, Table of Contents and/or a glossary of abbreviations or acronyms will not be included in the page count of the Technical Volume. However, be advised that any and all information contained within any Table of Contents and/or glossary of abbreviations or acronyms submitted with an Offeror’s proposal will not be evaluated by the Government.

See RFO 52.212-1, Instructions to Offerors – Commercial Items.

1. VOLUME I – TECHNICAL FACTOR.

a. The Offeror shall clearly demonstrate an understanding of the requirements by explaining how its proposed approach supports an enterprise-wide MTRS and meets the Clinical Functionality criteria below.

   1. Deliver a COTS solution that provides vendor-driven radiologist workflows incorporating API functionality with PACS and voice dictation systems. (PWS Section 5.2.6)

   2. Support multiple automated and manual trigger mechanisms for generating and transmitting Patient Lay Summary Letters. (PWS Section 5.2.8)

   3. Implement an AI calculation tool for a 5-year risk score in alignment with the most recent NCCN guidelines for breast cancer screening and diagnosis. (PWS Section 5.2.9.1)

   4. Develop user groups with distinct privileges and permissions. The Contractor shall describe the available default user groups in their Mammography Tracking System solution and the permissions/privileges assigned to each group. (PWS Section 5.8)

b. The Offeror's approach shall demonstrate its ability to install the MTS client software using a fully automated silent installer package, including the ability to apply software updates while retaining all user preferences, configurations, and customizations. The Offeror shall also describe the capabilities to implement the MTS solution within the VA Enterprise Cloud (VAEC) environment. (PWS Section 5.3)

c. The Offeror's approach shall include screenshots or appropriate documentation to demonstrate the following capabilities:

   1. A fully validated, bi-directional HL7 integration with both VistA and FEHR, supported by evidence of successful completion of VA's HL7 qualification processes to ensure interoperability and adherence to VA standards. (PWS section 5.9)

   2. Provide HL7 integration to VistA and OH Millenium and meet the qualification process for the VA VistA and OH Millenium HL7 interface. (PWS section 5.9)

   3. Provide DICOM Conformance Statements for all included products in the proposed Mammography Tracking System (MTS) solution. (PWS section 5.10)

   4. Demonstrate successful HL7 interface integration with the proposed Mammography Tracking System solution. (PWS section 5.9).

2. VOLUME II – PAST PERFORMANCE FACTOR

Offerors shall submit up to three (3) Federal instances (prime contracts, task/delivery orders, and/or major subcontracts) in performance at any point during the three (3) years immediately prior to the proposal submission date, which are relevant to the efforts required by this solicitation. Areas of relevance include integration, clinical workflow solution, data migration, interoperability, training, implementation, sustainment, and program management and execution of large-scale, multi-facility Mammography Tracking and Reporting system deployments within federal or complex healthcare environments. Data concerning the prime contractor shall be provided first, followed by each proposed major subcontractor, in alphabetical order. This volume shall be organized into the following sections:

a. Section 1 – Contract Descriptions. This section shall include the following information:

    1. Contractor/Subcontractor place of performance, CAGE Code and DUNS Number. If the work was performed as a subcontractor, also provide the name of the prime contractor and Point of Contact (POC) within the prime contractor organization (name, and current address, e-mail address, and telephone numbers).

    2. Contracting activity, and current address, Procuring Contracting Officer's name, e-mail address, and telephone numbers.

    3. Technical representative/Contracting Officer’s Representative (COR), and current e-mail address, and telephone numbers.

    4. Contract administration activity and the Administrative Contracting Officer's name, and current e-mail address, and telephone numbers.

    5. Contract Number, GSA contracts, and Blanket Purchase Agreements, include Delivery Order Numbers.

    6. Contract Type (specific type such as Fixed Price (FP), Cost Reimbursement (CR), Time & Materials (T&M), etc.).

    7. Awarded price.

    8. Final or projected final price.

    9. Original delivery schedule, including dates of start and completion of work.

    10. Final or projected final, delivery schedule, including dates of start and completion of work.

b. Section 2 - Performance. Offerors shall provide a specific narrative explanation of each contract listed in Section 1 describing the objectives achieved and detailing how the effort is relevant to the requirements of this solicitation. For any contract(s)/task

order(s) that did not/do not meet original schedule or technical performance requirements, provide a brief explanation of the reason(s) for the shortcoming(s) and any corrective action(s) taken to avoid recurrence. The Offerors shall list each time the delivery schedule was revised and provide an explanation of why the revision was necessary. The Offerors shall indicate if any of the contracts listed were terminated and the type and reasons for the termination.

c. Section 3 – Subcontracts. Offerors shall provide an outline of how the effort required by the solicitation will be assigned for performance within the Offeror's corporate entity and among the proposed subcontractors. The information provided for the prime Offeror and each proposed major subcontractor must include the entire company name, company address, CAGE Code, DUNS Number and type of work to be performed by citing the applicable Government PWS paragraph number.

d. Section 4 – New Corporate Entities. New corporate entities may submit data on prior contracts involving its officers and employees. However, in addition to the other requirements in this section, the Offeror shall discuss in detail the role performed by such persons in the prior contracts cited. Information should be included in the files described in the sections above.

e. Customer/Client Performance Risk Assessment Questionnaire:

A Past Performance Questionnaire prepared by the Offeror's Government customer/client for each of the Offeror's contract citations is required. The Offeror shall send the questionnaire electronically to the POCs for each Government contract/subcontract cited. It is the Offeror's responsibility to prepare and issue instructions with the questionnaire requesting that each customer/client complete their response and send it electronically directly to the Contract Specialist and Contracting Officer identified below by the time of proposal due date.

The Offeror shall specifically request that the Government customer/client prepare questionnaire response **NOT** be provided back to the Offeror, either as an original or as a copy. The Government POC(s) completed questionnaire shall be sent via e-mail to the Contract Specialist, Terricia Lloyd, Terricia.Lloyd@va.gov, and Contracting Officer Brett Schwerin, Brett.Schwerin@va.gov. The Offeror shall request that the Government POC(s) maintain the original completed/signed questionnaire as a record of their response.

3. VOLUME III – VETERANS INVOLVEMENT FACTOR.

a. For SDVOSBS/VOSBs: In order to receive credit under this Factor, an Offeror shall submit a statement of compliance that it qualifies as a SDVOSB or VOSB in accordance with VAAR 852.215-70, Service-Disabled Veteran-Owned and Veteran-Owned Small Business Evaluation Factors (DEVIATION). Offerors are cautioned that they must be registered and verified in Veteran Small Business Certification (VetCert) database (https://veterns.certify.sba.gov) and must meet federal small business size standards for the NAICS code assigned to this solicitation at time of both proposal submission and at time of award.

b. For Non-SDVOSBs/VOSBs: To receive some consideration under this Factor, an Offeror must state in its proposal the names of SDVOSB(s) and/or VOSB(s) with whom it intends to subcontract and provide a brief description and the approximate dollar values of the proposed subcontracts. Additionally, proposed SDVOSB/VOSB subcontractors must be registered and verified in the VetCert database (https://veterans.certify.sba.gov) in order to receive some consideration under the Veteran's Involvement Factor and must meet federal s all business size standards for the NAICS code assigned to this solicitation at time of both proposal submission and time of award.

4. VOLUME IV – PRICE FACTOR

The Offeror shall complete the Price Schedule found in solicitation, Section B5. Proposed unit prices shall be no more than two decimal places. These prices are binding as ceiling prices for each of the applicable ordering periods, regardless of the quantity being ordered. Calculation of the Total Evaluated FFP will be done by adding all items contained in the Price Schedule to arrive at the total FFP for the base, all option periods and optional tasks. All Offerors should propose using an estimated award date of September 30, 2026.
The Government will verify the Offeror's calculation of the total proposed price. Further, the Government may make adjustments to the evaluated price if mathematical errors are identified.

The Offeror shall complete B.5 Schedule of Supplies and Services and submit it as a Microsoft Word document titled 'Price Exhibit.' The Price Exhibit will be used for evaluation purposes and will be incorporated into the final award; therefore, the Offeror shall ensure that all unit prices, line items, and totals in the Price Exhibit are consistent with and accurately reflect the requirements of B.5 Schedule of Supplies and Services. .

Price Rounding Issue – The Government requires Offerors to propose unit prices and total prices that are two (2) decimal places and requires the unit prices and total prices to be displayed as two (2) decimal places. Ensure that the two (2) decimal unit price multiplied by the item quantity equals the two (2) decimal total item price, i.e., there should be no rounding. If an Excel spreadsheet is submitted by the Offerors, the Offerors shall ensure that the actual values in the spreadsheet cells are no more than two (2) decimal places even if values in the spreadsheet cells are formatted to display two (2) decimal places.

5. VOLUME V - SOLICITATION, OFFER AND AWARD DOCUMENTS AND CERTIFICATIONS/REPRESENTATIONS, SMALL BUSINESS SUBCONTRACTING PLAN (REQUIRED FOR LARGE BUSINESSES ONLY)

Certifications and Representations - An authorized official of the firm shall sign the SF 1449 and all certifications requiring original signature. An Acrobat PDF file shall be created to capture the signatures for submission. This Volume shall contain the following:

a. Solicitation Section A – Standard Form SF1449 and Acknowledgement of Amendments, if any.

b. Signed Business Associate Agreement.

c. Any proposed terms and conditions and/or assumptions upon which the proposal is predicated. Offerors are hereby advised that any Offeror-imposed terms and conditions and/or assumptions which deviate from the Government's material terms and conditions established by the Solicitation, may render the Offeror's proposal Unacceptable, and thus ineligible for award.

3. COMPETITIVE RANGE LIMITATION NOTICE

Offerors are advised that the Government may establish a competitive range in accordance with RFO 15.204 and VAAR Subpart 815. Following initial evaluation of proposals, if the Contracting Officer determines that the number of most highly rated proposals exceeds the level at which meaningful and manageable comparisons can be conducted, the competitive range may be limited to the greatest number of proposals that will support efficient and effective discussions. In accordance with VAAR 815.304-70, Offerors are reminded that evaluation may include preference for SDVOSB and VOSB participation. Offerors are therefore encouraged to submit initial proposals that fully demonstrate their technical capabilities, past performance, and SDVOSB/VOSB commitments. Only Offerors included in the competitive range will be invited to participate in discussions.

E.16 ARTIFICIAL INTELLIGENCE EFFORTS

Offerors shall, if Artificial Intelligence (AI) is part of the Contractor system/solution, provide the below self-certification with their quote/proposal affirming that the identified/proposed AI System/LLM complies with the two Unbiased AI Principles, Truth-seeking and Ideological Neutrality, as required by the Office of Management and Budget (OMB) Memorandum M-26-04, “Increasing Public Trust in Artificial Intelligence Through Unbiased AI Principles”, or indicate otherwise that a self-certification is Not Applicable. Additionally, Offerors shall self-certify that the content requested within the AI System/LLM Development and Operation Documentation Package, as identified in OMB Memorandum M-26-04 as Transparency Documentation, will be provided for its proposed AI System/LLM during the period of performance, meet the required transparency threshold and align with the two Unbiased AI Principles. Failure to include the requisite Offeror’s self-certification may render the Offeror’s proposal/quotation unacceptable, and therefore ineligible for award. The Government will rely on the Offeror’s self-certification that its proposed AI System/LLM adheres to the Unbiased AI Principles and related requirements. VA reserves the right to request additional information if it determines that doing so is in the Government’s best interest.

Certification:

☐ Not Applicable.
☐ I hereby certify that the proposed AI System/LLM complies with the required

Unbiased AI Principles as identified in OMB Memorandum M-26-04 and can also meet the required AI System/LLM Development and Operation Documentation requirements specified therein. I further certify that I am authorized to execute this certification on behalf of (*insert name of Offeror)* _____.

Printed Name of Signee: _____

Printed Title of Signee: _____

Signature: _____

Name (and version) of its proposed AI System/LLM: _____
_____

Date: _____

Company Name and Address: _____
_____