SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NO.

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NO.	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
			36C10B26Q0394	6/26/26

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NO. (No Collect Calls)	8. OFFER DUE DATE/LOCAL TIME
	Michelle Policari, Contract Specialist	848-377-5130	06-29-2026 1400 EDT

9. ISSUED BY CODE

Department of Veterans Affairs
Office of Procurement, Acquisition and Logistics
Technology Acquisition Center
23 Christopher Way, Eatontown, NJ 07724

10. THIS ACQUISITION IS

- [X] UNRESTRICTED OR
- [ ] SET ASIDE: _____ % FOR:
- [ ] SMALL BUSINESS
- [ ] HUBZONE SMALL BUSINESS
- [ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
- [ ] WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
- [ ] EDWOSB
- [ ] 8(A)

NAICS: 513210

SIZE STANDARD: $47 Million

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED

- [ ] SEE SCHEDULE

12. DISCOUNT TERMS

- [ ] 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)

13b. RATING: N/A

14. METHOD OF SOLICITATION

- [X] RFQ
- [ ] IFB
- [ ] RFP

15. DELIVER TO CODE

See Product Description

16. ADMINISTERED BY CODE 36C10B

Department of Veterans Affairs
Office of Procurement, Acquisition and Logistics
Technology Acquisition Center
23 Christopher Way Eatontown NJ 07724

17a. CONTRACTOR/OFFEROR CODE FACILITY CODE

TELEPHONE NO. UEI: EFT:

- [ ] 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18a. PAYMENT WILL BE MADE BY CODE

Department of Veterans Affairs
Financial Services Center
PO Box 149971 Austin TX 78714-8971
See website at: http://www.fsc.va.gov/einvoice.asp.

PHONE: (877) 353-979 FAX:

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED

- [ ] SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES (See CONTINUATION Page)	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	This effort is for: Brand Name Medicom Imagex with Assistant Software Subscriptions with Support This Request of Quote (RFQ) will result in a Firm Fixed Priced Contract. This effort is subject to the implementation of the class Deviation of the Revolutionary FAR Overhaul. The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause or provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause/provision. See rest of solicitation for requirements. Points of Contact: Contract Specialist: Michelle.Policari@va.gov Contracting Officer: Michael.Weckesser@va.gov (Use Reverse and/or Attach Additional Sheets as Necessary)				

25. ACCOUNTING AND APPROPRIATION DATA See CONTINUATION Page

26. TOTAL AWARD AMOUNT (For Govt. Use Only)

- [x] 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA [X] ARE [ ] ARE NOT ATTACHED.
- [ ] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED

- [ ] 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN _____ COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED

- [ ] 29. AWARD OF CONTRACT: REF. _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR

31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)

30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT) 30c. DATE SIGNED

31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT)
Michael Weckesser
Contracting Officer

31c. DATE SIGNED

Table of Contents

SECTION A **1**

A.1 SF 1449 SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES 1

SECTION B - CONTINUATION OF SF 1449 BLOCKS **4**

B.1 GOVERNING LAW CLAUSE 4
B.2 SOFTWARE LICENSE, SOFTWARE MAINTENANCE AND SOFTWARE TECHNICAL SUPPORT 5
B.3 CONTRACT ADMINISTRATION DATA 10
B.4 PRICE SCHEDULE 11
B.5 PRODUCT DESCRIPTION 19

ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/ PRIVACY LANGUAGE **29**

SECTION C - CONTRACT CLAUSES **43**

C.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998) 43
C.2 52.203-6 RESTRICTIONS ON SUBCONTRACTOR SALES TO THE GOVERNMENT (JUN 2020) 44
C.4 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000) 44
C.5 52.222-35 EQUAL OPPORTUNITY FOR VETERANS (DEVIATION NOV 2025) 45
C.6 52.222-36 EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES (DEVIATION NOV 2025) 45
C.7 52.222-37 EMPLOYMENT REPORTS ON VETERANS (DEVIATION NOV 2025) 46
C.9 52.229-12 TAX ON CERTAIN FOREIGN PROCUREMENTS (DEVIATION SEP 2025) 47
C.10 52.233-3 PROTEST AFTER AWARD (DEVIATION NOV 2025) 49
C.11 VAAR 852.201-70 CONTRACTING OFFICER'S REPRESENTATIVE (DEC 2022) 50
C.12 VAAR 852.203-70 COMMERCIAL ADVERTISING (MAY 2018) 50
C.13 VAAR 852.204-70 PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL (DEVIATION) (MAR 2026) 50
C.14 VAAR 852.204-71 INFORMATION AND INFORMATION SYSTEMS SECURITY (FEB 2023) 50
C.15 VAAR 852.204-72 PERSONNEL VETTING AND CREDENTIALING (MARCH 2026) 61
C.16 VAAR 852.222-71 COMPLIANCE WITH EXECUTIVE ORDER 13899 (DEVIATION)(APR 2025) 63
C.17 VAAR 852.232-72 ELECTRONIC SUBMISSION OF PAYMENT REQUESTS (NOV 2018) 64
C.18 VAAR 852.239-70 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES (FEB 2023) 65
C.19 VAAR 852.239-76 INFORMATION AND COMMUNICATIONS TECHNOLOGY ACCESSIBILITY (FEB 2023) 68
C.20 ARTIFICIAL INTELLIGENCE IN VA CONTRACTS (MAR 2026) 69

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS.....72

THIS PAGE INTENTIONALLY LEFT BLANK 72

SECTION E - SOLICITATION PROVISIONS.....73

E.1 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998) 73
E.2 52.216-1 TYPE OF CONTRACT (DEVIATION NOV 2025) 73
E.3 52.219-1 SMALL BUSINESS PROGRAM REPRESENTATIONS (DEVIATION NOV 2025) 74
E.4 52.229-11 TAX ON CERTAIN FOREIGN PROCUREMENTS—NOTICE AND REPRESENTATION (DEVIATION NOV 2025) 78
E.5 52.233-2 SERVICE OF PROTEST (DEVIATION NOV 2025) 79
E.6 52.240-90 SECURITY PROHIBITIONS AND EXCLUSIONS REPRESENTATIONS AND CERTIFICATIONS (DEVIATION NOV 2025).....80
E.7 VAAR 852.233-70 PROTEST CONTENT/ALTERNATIVE DISPUTE RESOLUTION (OCT 2018) 84
E.8 VAAR 852.233-71 ALTERNATE PROTEST PROCEDURE (OCT 2018).....85
E.9 VAAR 852.239-71 INFORMATION SYSTEM SECURITY PLAN AND ACCREDITATION (FEB 2023).....85
E.10 VAAR 852.239-75 INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY NOTICE (FEB 2023).....85
E.11 ARTIFICIAL INTELLIGENCE EFFORTS (MAR 2026) 86
E.11 BASIS FOR AWARD 87
E.12 QUOTE SUBMISSION INSTRUCTIONS 87

SECTION B - CONTINUATION OF SF 1449 BLOCKS

B.1 GOVERNING LAW CLAUSE

Federal law and regulations, including the Revolutionary Federal Acquisition Regulations (FAR) Overhaul (RFO), 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 (shrinkwrap), 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 RFO 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 RFO 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.2 SOFTWARE LICENSE, SOFTWARE MAINTENANCE AND SOFTWARE 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.

f) 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 RFO 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(e).
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(e); 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.3 CONTRACT ADMINISTRATION DATA

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

a. CONTRACTOR: TBD

b. GOVERNMENT: Contracting Officer 36C10B
Michael Weckesser
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] Upon acceptance of Deliverables in accordance with Section B.4, Price Schedule

4. GOVERNMENT INVOICE ADDRESS: All Invoices from the contractor shall be submitted electronically. Invoices meeting an exception in accordance with VAAR Clause 852.232-72 shall be mailed to the following address:

Department of Veterans Affairs
Financial Services Center
PO Box 149971
Austin TX 78714-8971

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

AMENDMENT NO	DATE

B.4 PRICE SCHEDULE

NOTE: Offeror shall complete Section B.4, Schedule of Supplies and Services and submit with its quote. Note: Alterations to the line items as specified below may render quotes unacceptable. All questions must be submitted via email to the Contract Specialist, prior to the closing date and time specified in the RFQ.

Any resulting contract will be awarded on a firm-fixed-price basis as defined by RFO Federal Acquisition Regulation (FAR) Subpart 16.202. 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.

All deliverables are as follows:

Inspection: Destination
Acceptance: Destination
Free on Board (FOB): Destination

Base Period				
CLIN	**Description**	**QTY**	**Unit Price**	**Total Price**
0001	**Imagex with Assistant Edition Software (Medical Image Exchange System) in accordance with (IAW) Product Description, B.5.** PSC Code: DA10 Period of Performance: July 1, 2026 thru June 30, 2027	10 EA	$_____	$_____
0002	**Support Services, Maintenance, and Training Agreement IAW Product Description, B.5.** PSC Code: DA10	10 EA	$_____	$_____

Base Period				
CLIN	**Description**	**QTY**	**Unit Price**	**Total Price**
	PoP: July 1, 2026 thru June 30, 2027			
0003	**AI System/LLM Development and Operation Documentation Package in accordance with Section B.5, Product Description Section 5.7.1.** To be submitted electronically to the VA Contracting Officers Representative (COR). Due within 3 days after contract award and updated ad hoc thereafter	1 LT	Not Separately Priced (NSP)	NSP
0004	**Compliance Monitoring and Reporting Plan IAW Section B.5, Product Description Section 5.7.2.** To be submitted electronically to the VA COR. Due within 3 days after contract award and updated ad hoc thereafter	1 LT	NSP	NSP
0005	**Corrective Action Plan IAW Section B.5, Product Description Section 5.7.2.** To be submitted electronically to the VA COR. Each Plan is due within 10 days of identifying a deviation to the Compliance Monitoring and Reporting Plan.	1 LT	NSP	NSP

Base Period				
CLIN	**Description**	**QTY**	**Unit Price**	**Total Price**
0006	**AI Model/LLM Change Disclosure IAW Section B.5, Product Description Section 5.7.3.** To be submitted electronically to the VA COR. Due within 3 days after contract award and updated ad hoc thereafter	1 LT	NSP	NSP
0007	**Contractor Staff Roster IAW Product Description, B.5.** To be submitted electronically to the VA COR. Due within 3 days after contract award and updated ad hoc thereafter	1 LT	NSP	NSP
			Total Base Period:	$_____

Option Period 1				
This 12-month option period may be exercised in accordance with FAR 52.217-9, Option to Extend the Term of the Contract (MAR 2000). Work shall not commence until, and unless, a formal modification is issued by the Contracting Officer. If exercised, this option shall commence at the end of the base period.				
CLIN	**Description**	**QTY**	**Unit Price**	**Total Price**
1001	**Imagex with Assistant Edition Software (Medical Image Exchange System) in accordance with (IAW) Product Description, B.5.**	10 EA	$_____	$_____

Option Period 1 This 12-month option period may be exercised in accordance with FAR 52.217-9, Option to Extend the Term of the Contract (MAR 2000). Work shall not commence until, and unless, a formal modification is issued by the Contracting Officer. If exercised, this option shall commence at the end of the base period.				
CLIN	**Description**	**QTY**	**Unit Price**	**Total Price**
	PSC Code: DA10 Period of Performance (PoP) shall be 12 months from date of option exercise			
1002	**Support Services, Maintenance, and Training Agreement IAW Product Description, B.5.** PSC Code: DA10 Period of Performance (PoP) shall be 12 months from date of option exercise	10 EA	$_____	$_____
1003	**AI System/LLM Development and Operation Documentation Package in accordance with Section B.5, Product Description Section 5.7.1.** **To be submitted electronically to the VA Contracting Officers Representative (COR).** To be updated ad hoc	1 LT	Not Separately Priced (NSP)	NSP
1004	**Compliance Monitoring and Reporting Plan IAW Section B.5, Product Description Section 5.7.2.** To be submitted electronically to the VA COR.	1 LT	NSP	NSP

Option Period 1 This 12-month option period may be exercised in accordance with FAR 52.217-9, Option to Extend the Term of the Contract (MAR 2000). Work shall not commence until, and unless, a formal modification is issued by the Contracting Officer. If exercised, this option shall commence at the end of the base period.				
CLIN	**Description**	**QTY**	**Unit Price**	**Total Price**
	To be updated ad hoc			
1005	**Corrective Action Plan IAW Section B.5, Product Description Section 5.7.2.** To be submitted electronically to the VA COR. Each Plan is due within 10 days of identifying a deviation to the Compliance Monitoring and Reporting Plan.	1 LT	NSP	NSP
1006	**AI Model/LLM Change Disclosure IAW Section B.5, Product Description Section 5.7.3.** To be submitted electronically to the VA COR. To be updated ad hoc	1 LT	NSP	NSP
1007	**Contractor Staff Roster IAW Product Description, B.5.** To be submitted electronically to the VA COR. To be updated ad hoc	1 LT	NSP	NSP
			Total Option Period 1:	$_____

Option Period 2 This 12-month option period may be exercised in accordance with FAR 52.217-9, Option to Extend the Term of the Contract (MAR 2000). Work shall not commence until, and unless, a formal modification is issued by the Contracting Officer. If exercised, this option shall commence at the end of the Option Period 1.				
CLIN	**Description**	**QTY**	**Unit Price**	**Total Price**
2001	**Imagex with Assistant Edition Software (Medical Image Exchange System) in accordance with (IAW) Product Description, B.5.** PSC Code: DA10 Period of Performance (PoP) shall be 12 months from date of option exercise	10 EA	$_____	$_____
2002	**Support Services, Maintenance, and Training Agreement IAW Product Description, B.5.** PSC Code: DA10 Period of Performance (PoP) shall be 12 months from date of option exercise	10 EA	$_____	$_____
2003	**AI System/LLM Development and Operation Documentation Package in accordance with Section B.5, Product Description Section 5.7.1.** **To be submitted electronically to the VA Contracting Officers Representative (COR).** To be updated ad hoc	1 LT	Not Separately Priced (NSP)	NSP
2004	**Compliance Monitoring and Reporting Plan IAW Section B.5,**	1 LT	NSP	NSP

Option Period 2 This 12-month option period may be exercised in accordance with FAR 52.217-9, Option to Extend the Term of the Contract (MAR 2000). Work shall not commence until, and unless, a formal modification is issued by the Contracting Officer. If exercised, this option shall commence at the end of the Option Period 1.				
CLIN	**Description**	**QTY**	**Unit Price**	**Total Price**
	Product Description Section 5.7.2. To be submitted electronically to the VA COR. To be updated ad hoc			
2005	**Corrective Action Plan IAW Section B.5, Product Description Section 5.7.2.** To be submitted electronically to the VA COR. Each Plan is due within 10 days of identifying a deviation to the Compliance Monitoring and Reporting Plan.	1 LT	NSP	NSP
2006	**AI Model/LLM Change Disclosure IAW Section B.5, Product Description Section 5.7.3.** To be submitted electronically to the VA COR. To be updated ad hoc	1 LT	NSP	NSP
2007	**Contractor Staff Roster IAW Product Description, B.5.** To be submitted electronically to the VA COR. To be updated ad hoc	1 LT	NSP	NSP

Option Period 2				
This 12-month option period may be exercised in accordance with FAR 52.217-9, Option to Extend the Term of the Contract (MAR 2000). Work shall not commence until, and unless, a formal modification is issued by the Contracting Officer. If exercised, this option shall commence at the end of the Option Period 1.				
CLIN	**Description**	**QTY**	**Unit Price**	**Total Price**
			Total Option Period 2:	$_____
			Total Contract Value	$_____

B.5 PRODUCT DESCRIPTION

1.0 PRODUCT REQUIREMENTS

VA, Veterans Health Administration (VHA), Veterans Integrated Service Network (VISN) 2 has a requirement for brand name Medicom Imagex with Assistant Edition software subscriptions per site (quantity of 10), associated support services, maintenance and training. VA requires a system that will satisfy the functional capability to save diagnostic images to the current VA systems and pathways, and both authenticate and validate bi-directional, electronic exchange of Digital Imaging and Communications in Medicine (DICOM) images, radiology reports, and radiology images. with commercial healthcare facilities providing services to VA patients. Specifically, this solution will provide a peer-to-peer network which enables the seamless and secure sharing of radiology information, including reports and images, through encrypted conduits between providers on a fully federated health information network. This requirement is for the Support Services, Maintenance, and Training of Medicom Imagex at ten sites within VISN 2. The associated maintenance support includes timely provision of patches and updates to ensure the software remains operational, and virtual training will be provided to ensure seamless coordination with product updates. The Contractor shall coordinate with the VA Contracting Officer's Representative (COR) to coordinate training schedule/times, and shall furnish all necessary training materials and provide training to the VA as required The period of performance shall be one 12-month base period with two 12-month option periods for continued access to the Medicom Imagex subscription, associated maintenance and support.

This requirement for the Medicom Imagex at 10 VA Medical Centers and VA Healthcare Systems within VISN 2, as follows:

6 VAMCS
- Albany Stratton VAMC
- Bath VAMC
- Bronx VAMC
- Canandaigua VAMC
- Northport VAMC
- Syracuse VAMC

4 VA Healthcare Systems
- VA Hudson Valley Healthcare System
- VA New Jersey Healthcare System
- VA New York Harbor Healthcare System
- VA Western New York Healthcare System

The Contract Holder shall provide the following in the base and each option period, if exercised:

Description:

Brand Name Product	Quantity

Imagex with Assistant Edition Software (Medical Image Exchange System)	10
Support Services, Maintenance, and Training Agreement	10

2.0 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.

2.1 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

2.2 COMPATABILITY 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.

2.3 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.

3.0 INFORMATION TECHNOLOGY USING SUSTAINABLE PRODUCTS

4.0 SHIPMENT OF HARDWARE OR EQUIPMENT

N/A

4.1 SPECIAL SHIPPING INSTRUCTIONS

N/A

4.2 NATIONAL ACQUISITIONS

N/A

5.0 GENERAL REQUIREMENTS

5.1 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.

5.2 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.

5.3 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 Integrated Control Number (ICN) in all VA information systems for all individuals. The Contractor shall ensure that all Contractor delivered applications and systems integrate with the VA Master Person Index (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.

5.4 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.

5.5 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.

5.6 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.)

5.7 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.

No web-based, publicly available generative AI service has been approved for use with VA-sensitive data including, but not limited to OpenAI's ChatGPT, Microsoft's Copilot, Google's Gemini, and Anthropic's Claude. No PII, protected health information (PHI), or VA-sensitive data should be entered into these unapproved services. The entire definition of VA Sensitive Data can be found at 38 U.S.C. § 5727 (23). 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.

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:

A. Statement of Attestation

5.7.1 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.

Deliverable:

A. AI System/LLM Development and Operation Documentation Package

5.7.2 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.

Deliverable:

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

5.7.3 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

6.0 SECURITY AND PRIVACY REQUIREMENTS

6.1 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 PD are:

Position Sensitivity and Background Investigation Requirements by Service Task/Item Number

Service Task / Item Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
1.0	☐	☐	☒

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 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:

A. Contractor Staff Roster

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 N/A

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)
N/A

B14. DATA CENTER PROVISIONS

a. 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.

b. 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.

c. 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).

d. 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.

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

f. 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.

INFORMATION SECURITY CONSIDERATIONS

All VA sensitive information shall be protected at all times in accordance with 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 Product Description.

7. POINTS OF CONTACT:

VA Program Manager:
Name: Provided Award
Address:
Voice:
Email:

Contracting Officer's Representative:
Name: Provided Award
Address:
Voice:
Email:

Contracting Officer:
Name: Michael Weckesser
Address: 23 Christopher Way Eatontown NJ 07724
Voice: 848-377-5052
Email: Michael.Weckesser@va.gov

Contract Specialist:
Name: Michelle Policari
Address: 23 Christopher Way Eatontown NJ 07724
Voice: 848-377-5130
Email: Michelle.Policari@va.gov

SECTION C - CONTRACT CLAUSES

C.1 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):

http://www.acquisition.gov/far/index.html
http://www.va.gov/oamm/oa/ars/policyreg/vaar/index.cfm
https://www.acquisition.gov/far-overhaul

FAR Number	Title	Date
52.203-3	GRATUITIES	APR 1984
52.203-12	LIMITATION ON PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS	JUN 2020
52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS	NOV 2023
52.203-19	PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS	JAN 2017
52.204-9	PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL	JAN 2011
52.204-19	INCORPORATION BY REFERENCE OF REPRESENTATIONS AND CERTIFICATIONS.	DEC 2014
52.209-6	PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, PROPOSED FOR DEBARMENT, OR VOLUNTARILY EXCLUDED	NOV 2025 (DEVIATION)
52.209-9	PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL	NOV 2025 (DEVIATION)
52.209-10	PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC COPRORATIONS	NOV 2025 (DEVIATION)
52.212-4	CONTRACT TERMS AND CONDITIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES	OCT 2025 (DEVIATION)
52.219-8	UTILIZATION OF SMALL BUSINESS CONCERNS	NOV 2025 (DEVIATION)
52.219-28	POSTAWARD SMALL BUSINESS PROGRAM REPRESENTATION	NOV 2025 (DEVIATION)
52.222-3	CONVICT LABOR	NOV 2025 (DEVIATION)
52.222-40	NOTIFICATION OF EMPLOYEE RIGHTS UNDER THE NATIONAL LABOR RELATIONS ACT	NOV 2025 (DEVIATION)
52.222-50	COMBATTING TRAFFICKING IN PERSONS (DEVIATION)	NOV 2025 (DEVIATION)

52.226-8	ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING	MAY 2024
52.222-90	ADDRESSING DEI DISCRIMINATION BY FEDERAL CONTRACTORS	APR 2026
52.227-1	AUTHORIZATION AND CONSENT	JUN 2020
52.227-2	NOTICE AND ASSISTANCE REGARDING PATENT AND COPYRIGHT INFRINGEMENT	JUN 2020
52.232-33	PAYMENT BY ELECTRONIC FUNDS TRANSFER-SYSTEM FOR AWARD MANAGEMENT	OCT 2018
52.232-40	PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS	MAR 2023
52.233-1	DISPUTES	NOV 2025 (DEVIATION)
52.233-4	APPLICABLE LAW FOR BREACH OF CONTRACT CLAIM	NOV 2025 (DEVIATION)
52.240-91	SECURITY PROHIBITIONS AND EXCLUSIONS (DEVIATION)	NOV 2025 (DEVIATION)
52.240-93	BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (DEVIATION)	NOV 2025 (DEVIATION)
52.242-13	BANKRUPTCY	JUL 1995

(End of Clause)

C.2 52.203-6 RESTRICTIONS ON SUBCONTRACTOR SALES TO THE GOVERNMENT (JUN 2020)

(a) Except as provided in (b) of this clause, the Contractor shall not enter into any agreement with an actual or prospective subcontractor, nor otherwise act in any manner, which has or may have the effect of restricting sales by such subcontractors directly to the Government of any item or process (including computer software) made or furnished by the subcontractor under this contract or under any follow-on production contract.

(b) The prohibition in (a) of this clause does not preclude the Contractor from asserting rights that are otherwise authorized by law or regulation.

(c) The Contractor agrees to incorporate the substance of this clause, including this paragraph (c), in all subcontracts under this contract which exceed the simplified acquisition threshold, as defined in Federal Acquisition Regulation 2.101 on the date of subcontract award.

(End of clause)

C.4 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 prior to the expiration of the contract; 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 36 months.

(End of clause)

C.5 52.222-35 EQUAL OPPORTUNITY FOR VETERANS (DEVIATION NOV 2025)

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

"Active duty wartime or campaign badge veteran," "Armed Forces service medal veteran," "disabled veteran," "protected veteran," "qualified disabled veteran," and "recently separated veteran" have the meanings given at Federal Acquisition Regulation (FAR) 22.1301.

(b) Equal opportunity requirements. The Contractor must abide by the requirements of 38 U.S.C. 4212(a)(1) and (2). These requirements prohibit discrimination against qualified protected veterans, and requires affirmative action by the Contractor to employ and advance in employment qualified protected veterans.

(c) Subcontracts. The Contractor must insert the terms of this clause in subcontracts valued at or above the threshold specified in FAR 22.1302-1(a)(2) on the date of subcontract award, unless exempted by rules, regulations, or orders of the Secretary of Labor. The Contractor must act as specified by the Director, Office of Federal Contract Compliance Programs, to enforce the terms, including action for noncompliance. Such necessary changes in language may be made as shall be appropriate to identify properly the parties and their undertakings.

(End of clause)

C.6 52.222-36 EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES (DEVIATION NOV 2025)

(a) Equal opportunity clause. The Contractor must abide by the requirements of the equal opportunity clause at 41 CFR 60-741.5(a), as of March 24, 2014. This clause prohibits discrimination against qualified individuals on the basis of disability, and requires affirmative action by the Contractor to employ and advance in employment qualified individuals with disabilities.

(b) Subcontracts. The Contractor must include the terms of this clause in every subcontract or purchase order in excess of the threshold specified in Federal Acquisition Regulation (FAR) 22.1401-2(a)(1) on the date of subcontract award, unless

exempted by rules, regulations, or orders of the Secretary, so that such provisions will be binding upon each subcontractor or vendor. The Contractor must act as specified by the Director, Office of Federal Contract Compliance Programs of the U.S. Department of Labor, to enforce the terms, including action for noncompliance. Such necessary changes in language may be made as shall be appropriate to identify properly the parties and their undertakings.

(End of clause)

C.7 52.222-37 EMPLOYMENT REPORTS ON VETERANS (DEVIATION NOV 2025)

(a) *Definitions.* As used in this clause, "active duty wartime or campaign badge veteran," "Armed Forces service medal veteran," "disabled veteran," "protected veteran," and "recently separated veteran," have the meanings given in Federal Acquisition Regulation (FAR) 22.1301.

(b) Unless the Contractor is a State or local government agency, the Contractor must report at least annually, as required by the Secretary of Labor, on-

(1) The total number of employees in the contractor's workforce, by job category and hiring location, who are protected veterans (*i.e.*, active duty wartime or campaign badge veterans, Armed Forces service medal veterans, disabled veterans, and recently separated veterans);

(2) The total number of new employees hired during the period covered by the report, and of the total, the number of protected veterans (*i.e.*, active duty wartime or campaign badge veterans, Armed Forces service medal veterans, disabled veterans, and recently separated veterans); and

(3) The maximum number and minimum number of employees of the Contractor or subcontractor during the period covered by the report.

(c) The Contractor must report the above items by filing the VETS-4212 "Federal Contractor Veterans' Employment Report" (see "VETS-4212 Federal Contractor Reporting" and "Filing Your VETS-4212 Report" at http://www.dol.gov/vets/vets4212.htm).

(d) The Contractor must file VETS-4212 Reports no later than September 30 of each year.

(e) The employment activity report required by paragraphs (b)(2) and (b)(3) of this clause must reflect total new hires, and maximum and minimum number of employees, during the most recent 12–month period preceding the ending date selected for the report.

(f) The number of veterans reported must be based on data known to the contractor when completing the VETS-4212. The contractor's knowledge of veterans status may

be obtained in a variety of ways, including an invitation to applicants to self-identify (in accordance with 41 CFR 60-300.42), voluntary self-disclosure by employees, or actual knowledge of veteran status by the contractor. This paragraph does not relieve an employer of liability for discrimination under 38 U.S.C. 4212.

(g) The Contractor must insert the terms of this clause in subcontracts valued at or above the threshold specified in FAR 22.1302-1(b) on the date of subcontract award, unless exempted by rules, regulations, or orders of the Secretary of Labor.

(End of clause)

C.9 52.229-12 TAX ON CERTAIN FOREIGN PROCUREMENTS (DEVIATION SEP 2025)

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

Foreign person means any person other than a United States person.

United States person, as defined in 26 U.S.C. 7701(a)(30), means–

(1) A citizen or resident of the United States;

(2) A domestic partnership;

(3) A domestic corporation;

(4) Any estate (other than a foreign estate, within the meaning of 26 U.S.C. 7701(a)(31)); and

(5) Any trust if-

(i) A court within the United States is able to exercise primary supervision over the administration of the trust; and

(ii) One or more United States persons have the authority to control all substantial decisions of the trust.

(b) This clause applies only to foreign persons. It implements 26 U.S.C. 5000C and its implementing regulations at 26 CFR 1.5000C-1 through 1.5000C-7.

(c)

(1) If the Contractor is a foreign person and has only a partial or no exemption to the withholding, the Contractor shall include the Department of the Treasury IRS Form W-14, Certificate of Foreign Contracting Party Receiving Federal Procurement Payments, with each voucher or invoice submitted under this contract throughout the period in which this status is applicable. The excise tax withholding is applied at the payment level, not at the contract level. The Contractor should revise each IRS Form W-14

submission to reflect the exemption (if any) that applies to that particular invoice, such as a different exemption applying. In the absence of a completed IRS Form W-14 accompanying a payment request, the default withholding percentage is 2 percent for the section 5000C withholding for that payment request. Information about IRS Form W-14 and its separate instructions is available via the internet at www.irs.gov/w14.

(2) If the Contractor—

(i) Is a foreign person; and

(ii) Has indicated in its offer in the provision 52.229-11, Tax on Certain Foreign Procurements—Notice and Representation, that it is fully exempt from the withholding; and

(iii) Certified the full exemption on the IRS Form W-14, and if that full exemption no longer applies due to a change in circumstances during the performance of the contract that causes the Contractor to become subject to the withholding for the 2 percent excise tax; then the Contractor shall–

(A) Notify the Contracting Officer within 30 days of a change in circumstances that causes the Contractor to be subject to the excise tax withholding under 26 U.S.C. 5000C; and

(B) Comply with paragraph (c)(1) of this clause.

(d) The Government will withhold a full 2 percent of each payment unless the Contractor claims an exemption. If the Contractor enters a ratio in Line 12 of the IRS Form W-14, the result of Line 11 divided by Line 10, the Government will withhold from each payment an amount equal to 2 percent multiplied by the contract ratio. If the Contractor marks box 9 of the IRS Form W-14 (rather than completes Lines 10 through 12), the Contractor must identify and enter the specific exempt and nonexempt amounts in Line 15 of the IRS Form W-14; the Government will then withhold 2 percent only from the nonexempt amount. See the IRS Form W-14 and its instructions.

(e) Exemptions from the withholding under this clause are described at 26 CFR 1.5000C-1(d)(5) through (7). Any exemption claimed and self-certified on the IRS Form W-14 is subject to audit by the IRS. Any disputes regarding the imposition and collection of the 26 U.S.C. 5000C tax are adjudicated by the IRS as the 26 U.S.C. 5000C tax is a tax matter, not a contract issue.

(f) Taxes imposed under 26 U.S.C. 5000C may not be—

(1) Included in the contract price; nor

(2) Reimbursed.

(g) A taxpayer may, for a fee, seek advice from the IRS as to the proper tax treatment of a transaction. This is called a private letter ruling. Also, the IRS may publish a revenue ruling, which is an official interpretation by the IRS of the Internal Revenue Code, related statutes, tax treaties, and regulations. A revenue ruling is the conclusion of the IRS on how the law is applied to a specific set of facts. For questions relating to the interpretation of the IRS regulations go to https://www.irs.gov/help/tax-law-questions.

(End of clause)

C.10 52.233-3 PROTEST AFTER AWARD (DEVIATION NOV 2025)

(a) Upon receipt of a stop-work order, the Contractor must immediately comply with its terms and take all reasonable steps to minimize incurring costs allocable to the work covered by the order during the period of work stoppage. After receiving the final decision in the protest, the Contracting Officer must either—

(1) Cancel the stop-work order; or

(2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.

(b) If a stop-work order issued under this clause is canceled either before or after a final decision in the protest, the Contractor must resume work. The Contracting Officer must make an equitable adjustment in the delivery schedule or contract price, or both, and the contract must be modified, in writing, accordingly, if—

(1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and

(2) The Contractor asserts its right to an adjustment within 30 days after the end of the period of work stoppage; provided, that if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon a proposal submitted at any time before final payment under this contract.

(c) If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer must allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.

(d) If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer must allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

(e) The Government's rights to terminate this contract at any time are not affected by action taken under this clause.

(f) If, as the result of the Contractor's intentional or negligent misstatement, misrepresentation, or miscertification, a protest related to this contract is sustained, and

the Government pays costs, the Government may require the Contractor to reimburse the Government the amount of such costs. In addition to any other remedy available, and pursuant to the requirements of subpart 32.6, the Government may collect this debt by offsetting the amount against any payment due the Contractor under any contract between the Contractor and the Government.

(End of clause)

C.11 VAAR 852.201-70 CONTRACTING OFFICER'S REPRESENTATIVE (DEC 2022)

The Contracting Officer reserves the right to designate representatives to act for him/her in furnishing technical guidance and advice or generally monitor the work to be performed under this contract. Such designation will be in writing and will define the scope and limitation of the designee's authority. A copy of the designation letter shall be furnished to the Contractor.

(End of clause)

C.12 VAAR 852.203-70 COMMERCIAL ADVERTISING (MAY 2018)

The Contractor shall not make reference in its commercial advertising to Department of Veterans Affairs contracts in a manner that states or implies the Department of Veterans Affairs approves or endorses the Contractor's products or services or considers the Contractor's products or services superior to other products or services.

(End of clause)

C.13 VAAR 852.204-70 PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL (DEVIATION) (MAR 2026)

(a) The Contractor shall comply with current Department of Veterans Affairs policy for personal identity verification of all employees performing under this contract when physical access to VA facilities and/or logical access to VA information systems is required.

(b) The Contractor shall insert this clause in all subcontracts when the subcontractor's employees will require physical access to VA facilities and/or logical access to VA information systems.

(End of clause)

C.14 VAAR 852.204-71 INFORMATION AND INFORMATION SYSTEMS SECURITY (FEB 2023)

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

Business Associate means an entity, including an individual (other than a member of the workforce of a covered entity), company, organization or another covered entity, as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, that performs or assists in the performance of a function or activity on behalf of the Veterans Health Administration (VHA) that involves the creating, receiving, maintaining, transmitting of, or having access to, protected health information (PHI). The term also includes a subcontractor of a business associate that creates, receives, maintains, or transmits PHI on behalf of the business associate.

Business Associate Agreement (BAA) means the agreement, as dictated by the Privacy Rule, between VHA and a business associate, which must be entered into in addition to the underlying contract for services and before any release of PHI can be made to the business associate, in order for the business associate to perform certain functions or activities on behalf of VHA.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information whether automated or manual.

Information technology (see FAR 2.101) also means Information and Communication Technology (ICT).

Information technology-related contracts means those contracts which include services (including support services), and related resources for information technology as defined in 802.101.

Privacy officer means the VA official with responsibility for implementing and oversight of privacy related policies and practices that impact a given VA acquisition.

Sensitive personal information means, with respect to an individual, any information about the individual maintained by VA, including but not limited to the following:

(1) Education, financial transactions, medical history, and criminal or employment history.

(2) Information that can be used to distinguish or trace the individual's identity, including but not limited to name, social security number, date and place of birth, mother's maiden name, or biometric records.

Security plan means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.

VA Information Security Rules of Behavior for Organizational Users (VA National Rules of Behavior) means a set of VA rules that describes the responsibilities and expected behavior of users of VA information or information systems.

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*. Contractors, subcontractors, their employees, third-parties, and business associates with access to VA information, information systems, or information technology (IT) or providing and accessing IT-related goods and services, shall adhere to VA Directive 6500, VA Cybersecurity Program, and the directives and handbooks in the VA 6500 series related to VA information (including VA sensitive information and sensitive personal information and information systems security and privacy), as well as those set forth in the contract specifications, statement of work, or performance work statement. These include, but are not limited to, VA Handbook 6500.6, Contract Security; and VA Directive and Handbook 0710, Personnel Security and Suitability Program, which establishes VA's procedures, responsibilities, and processes for complying with current Federal law, Executive Orders, policies, regulations, standards and guidance for protecting VA information, information systems (see 802.101, Definitions) security and privacy, and adhering to personnel security requirements when accessing VA information or information systems.

(c) *Access to VA information and VA information systems*. (1) Contractors are limited in their request for logical or physical access to VA information or VA information systems for their employees, subcontractors, third parties and business associates to the extent necessary to perform the services or provide the goods as specified in the contracts, agreements, task, delivery or purchase orders.

(2) All Contractors, subcontractors, third parties, and business associates working with VA information are subject to the same investigative 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 to access VA information and VA information systems shall be in accordance with VA Directive and Handbook 0710, Personnel Security and Suitability Program.

(3) Contractors, subcontractors, third parties, and business associates who require access to national security programs must have a valid security clearance.

(4) *HIPAA Business Associate Agreement requirement*. Contractors shall enter into a Business Associate Agreement (BAA) with VHA, VA's Covered Entity, when contract requirements and access to protected health information is required and when requested by the Contracting Officer, or the Contracting Officer's Representative (COR) (see VAAR 824.103-70). Under the HIPAA Privacy and Security Rules, a Covered Entity (VHA) must have a satisfactory assurance that its PHI will be safeguarded from misuse. To do so, a Covered Entity enters into a BAA with a contractor (now the business associate), which obligates the business associate to only use the Covered Entity's PHI for the purposes for which it was engaged, provide the same protections and safeguards as is required from the Covered Entity, and agree to the same disclosure restrictions to PHI that is required of the Covered Entity in situations where a contractor—

(i) Creates, receives, maintains, or transmits VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI in order to perform certain health care operations activities or functions on behalf of the Covered Entity; or

(ii) Provides one or more of the services specified in the Privacy Rule to or for the Covered Entity.

(A) *Contractors or entities required to execute BAAs for contracts and other agreements become VHA business associates*. BAAs are issued by VHA or may be issued by other VA programs in support of VHA. The HIPAA Privacy Rule requires VHA to execute compliant BAAs with persons or entities that create, receive, maintain, or transmit VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI in order to perform certain activities, functions or services to, for, or on behalf of VHA. There may be other VA components or staff offices which also provide certain services and support to VHA and must receive PHI in order to do so. If these components award contracts or enter into other agreements, purchase/delivery orders, modifications and issue governmentwide purchase card transactions to help in the delivery of these services to VHA, they will also fall within the requirement to obtain a satisfactory assurance from these contractors by executing a BAA.

(B) *BAA requirement flow down to subcontractors*. A prime Contractor required to execute a BAA shall also obtain a satisfactory assurance, in the form of a BAA, that any of its subcontractors who will also create, receive, maintain, or transmit VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI will comply with HIPAA requirements to the same degree as the Contractor. Contractors employing a subcontractor who creates, receives, maintains, or transmits VHA PHI or that will store, generate, access, exchange, process, or utilize such VHA PHI under a contract or agreement is required to execute a BAA with each of its subcontractors which also obligates the subcontractor (i.e., also a business associate) to provide the same

protections and safeguards and agree to the same disclosure restrictions to VHA's PHI that is required of the Covered Entity and the prime Contractor.

(d) *Contractor operations required to be in United States*. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practicable. If such services are proposed to be performed outside the continental United States, and are not otherwise disallowed by other Federal law, regulations or policy, or other VA policy or other mandates as stated in the contract, specifications, statement of work or performance work statement (including applicable Business Associate Agreements), the Contractor/subcontractor must state in its proposal where all non-U.S. services are provided. At a minimum, the Contractor/subcontractor must include a detailed Information Technology Security Plan, for review and approval by the Contracting Officer, specifically to address mitigation of the resulting problems of communication, control, and data protection.

(e) *Contractor/subcontractor employee reassignment and termination notification*. Contractors and subcontractors shall provide written notification to the Contracting Officer and Contracting Officer's Representative (COR) immediately, and not later than four (4) hours, when an employee working on a VA information system or with access to VA information is reassigned or leaves the Contractor or subcontractor's employment on the cognizant VA contract. The Contracting Officer and COR must also be notified immediately by the Contractor or subcontractor prior to an unfriendly termination.

(f) *VA information custodial requirements*. (1) *Release, publication, and use of data*. Information made available to a Contractor or subcontractor by VA for the performance or administration of a contract or information developed by the Contractor/subcontractor in performance or administration of a contract shall be used only for the stated contract purpose and shall not be used in any other way without VA's prior written approval. This clause expressly limits the Contractor's/subcontractor's rights to use data as described in Rights in Data—General, FAR 52.227-14(d).

(2) *Media sanitization*. VA information shall not be co-mingled with any other data on the Contractors/subcontractor's information systems or media storage systems in order to ensure federal and VA requirements related to data protection, information segregation, classification requirements, and media sanitization can be met (see VA Directive 6500, VA Cybersecurity Program).VA reserves the right to conduct scheduled or unscheduled on-site inspections, assessments, or audits of Contractor and subcontractor IT resources, information systems and assets to ensure data security and privacy controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with Federal and VA requirements. The Contractor and subcontractor will provide all necessary access and support to VA and/or GAO staff during periodic control assessments or audits.

(3) *Data retention, destruction, and contractor self-certification*. The Contactor and its subcontractors are responsible for collecting and destroying any VA data provided,

created, or stored under the terms of this contract, to a point where VA data or materials are no longer readable or reconstructable to any degree, in accordance with VA Directive 6371, Destruction of Temporary Paper Records, or subsequent issue. Prior to termination or completion of this contract, the Contractor/subcontractor must provide its plan for destruction of all VA data in its possession according to VA Directive 6500, and VA Cybersecurity Program, including compliance with National Institute of Standards and Technology (NIST) 800-88, Guidelines for Media Sanitization, for the purposes of media sanitization on all IT equipment. The Contractor must certify in writing to the Contracting Officer within 30 days of termination of the contract that the data destruction requirements in this paragraph have been met.

(4) *Return of VA data and information*. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to the VA (as stipulated by the Contracting Officer or the COR) or the Contractor/subcontractor must hold it until otherwise directed. Items returned will be hand carried, securely mailed, emailed, or securely electronically transmitted to the Contracting Officer or to the address as provided in the contract or by the assigned COR, and/or accompanying BAA. Depending on the method of return, Contractor/subcontractor must store, transport, or transmit VA sensitive information, when permitted by the contract using VA-approved encryption tools that are, at a minimum, validated under Federal Information Processing Standards (FIPS) 140-3 (or its successor). If mailed, Contractor/subcontractor must send via a trackable method (USPS, UPS, Federal Express, etc.) and immediately provide the Contracting Officer with the tracking information.No information, data, documentary material, records or equipment will be destroyed unless done in accordance with the terms of this contract and the VHA Records Control Schedule 10-1.

(5) *Use of VA data and information*. The Contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies.If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if the National NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies for this contract as a result of any updates, if required.

(6) *Copying VA data or information*. The Contractor/subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the contract or to preserve electronic information stored on Contractor/subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/subcontractor needs to be restored to an operating state. If copies are

made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

(7) *Violation of information custodial requirements*. If VA determines that the Contractor has violated any of VA's information confidentiality, privacy, or security provisions, it shall be sufficient grounds for VA to withhold payment to the Contractor or third-party or terminate the contract for default in accordance with FAR part 49 or terminate for cause in accordance with FAR 12.403.

(8) *Encryption*. The Contractor/subcontractor must store, transport, or transmit VA sensitive information, when permitted by the contract, using cryptography, and VA-approved encryption tools that are, at a minimum, validated under FIPS 140-3 (or its successor).

(9) *Firewall and web services security controls*. The Contractor/subcontractor's firewall and web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.

(10) *Disclosure of VA data and information*. Except for uses and disclosures of VA information authorized in a cognizant contract for performance of the contract, the Contractor/subcontractor may use and disclose VA information only in two other situations: (i) subject to paragraph (f)(10) of this section, in response to a court order from a court of competent jurisdiction, or (ii) with VA's prior written approval. The Contractor/subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the Contracting Officer for response. If the Contractor/subcontractor is in receipt of a court order or other request or believes it has a legal requirement to disclose VA information, that Contractor/subcontractor shall immediately refer such court order or other request to the Contracting Officer for response. If the Contractor or subcontractor discloses information on behalf of VHA, the Contractor and/or subcontractor must maintain an accounting of disclosures. Accounting of Disclosures documentation maintained by the Contractor/subcontractor will include the name of the individual to whom the information pertains, the date of each disclosure, the nature or description of the information disclosed, a brief statement of the purpose of each disclosure or, in lieu of such statement, a copy of a written request for a disclosure, and the name and address of the person or agency to whom the disclosure was made. The Contractor/subcontractor will provide its Accounting of Disclosures upon request and within 15 calendar days to the assigned COR and Privacy Officer. Accounting of disclosures should be provided electronically via encrypted email to the COR and designated VA facility Privacy Officer as provided in the contract, BAA, or by the Contracting Officer. If providing the Accounting of Disclosures electronically cannot be done securely, the Contractor/subcontractor will provide copies via trackable methods (UPS, USPS, Federal Express, etc.) immediately, providing the designated COR and Privacy Officer with the tracking information.

(11) Compliance with privacy statutes and applicable regulations. The Contractor/subcontractor shall not disclose VA information protected by any of VA's privacy statutes or applicable regulations including but not limited to: the Privacy Act of 1974, 38 U.S.C. 5701, confidential nature of claims, 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus or the HIPAA Privacy Rule. If the Contractor/subcontractor is in receipt of a court order or other requests for VA information or has questions if it can disclose information protected under the above-mentioned confidentiality statutes because it is required by law, that Contractor/subcontractor shall immediately refer such court order or other request to the Contracting Officer for response.

(g) *Report of known or suspected security/privacy incident*. The Contractor, subcontractor, third-party affiliate or business associate, and its employees shall notify VA immediately via the Contracting Officer and the COR or within one (1) hour of an incident which is an occurrence (including the discovery or disclosure of successful exploits of system vulnerability) that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or the availability of its data and operations, or of its information or information system(s); or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. The initial notification may first be made verbally but must be followed up in writing within one (1) hour. See VA Data Breach Response Service at https://www.oprm.va.gov/dbrs/about_dbrs.aspx. Report all actual or suspected security/privacy incidents and report the information to the Contracting Officer and the COR as identified in the contract or as directed in the contract, within one hour of discovery or suspicion.

(1) Such issues shall be remediated as quickly as is practical, but in no event longer than five days The Contractor shall notify the Contracting Officer in writing.

(2) When the security fixes involve installing third party patched (e.g., Microsoft OS patches or Adobe Acrobat), the Contractor will provide written notice to VA that the patch has been validated as not affecting the systems within 10 working days. When the Contractor is responsible for operations or maintenance of the systems, they shall apply the security fixes within _30 days of discovery

(3) All other vulnerabilities shall be remediated in a timely manner based on risk, but within 60 days of discovery or disclosure. Contractors shall notify the Contracting Officer, and COR within 2 business days after remediation of the identified vulnerability. Exceptions to this paragraph (e.g., for the convenience of VA) must be requested by the Contractor through the COR and shall only be granted with approval of the Contracting Officer and the VA Assistant Secretary for Office of Information and Technology. These

exceptions will be tracked by the Contractor in concert with the Government in accordance with VA Directive 6500 and related VA Handbooks.

(h) *Security and privacy incident investigation*. (1) The term “privacy incident” means the unauthorized disclosure or use of VA information protected under a confidentiality statute or regulation.

(2) The term "security incident" means an occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information systems; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable policies. The Contractor/ subcontractor shall immediately notify the Contracting Officer and COR for the contract of any known or suspected security or privacy incident, or any other unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/subcontractor has access.

(3) To the extent known by the Contractor/subcontractor, the Contractor/ subcontractor's notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/subcontractor considers relevant.

(4) With respect to unsecured PHI, the Business Associate is deemed to have discovered a security incident as defined above when the Business Associate either knew, or by exercising reasonable diligence should have been known to an employee of the Business Associate. Upon discovery, the Business Associate must notify VHA of the security incident immediately within one hour of discovery or suspicion as agreed to in the BAA.

(5) 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.

(i) *Data breach notification requirements*. (1) This contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach involving any VA sensitive personal information the Contractor/Subcontractor processes or maintains under the contract as set forth in clause 852.211-76, Liquidated Damages—Reimbursement for Data Breach Costs.

(2) The Contractor/subcontractor shall provide notice to VA of a privacy or security incident as set forth in the Security and Privacy Incident Investigation section of this clause. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. The Contractor 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.

(3) The Contractor/subcontractor shall fully cooperate with VA or any Government agency conducting an analysis regarding any notice of a data breach or potential data breach or security incident which may require the Contractor to provide information to the Government or third-party performing a risk analysis for VA, and shall address all relevant information concerning the data breach, including the following:

(i) Nature of the event (loss, theft, unauthorized access).

(ii) Description of the event, including—

(A) Date of occurrence;

(B) Date of incident detection;

(C) Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code.

(D) Number of individuals affected or potentially affected.

(E) Names of individuals or groups affected or potentially affected.

(F) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text.

(G) Amount of time the data has been out of VA control.

(H) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons).

(I) Known misuses of data containing sensitive personal information, if any.

(J) Assessment of the potential harm to the affected individuals.

(K) Data breach analysis as outlined in 6500.2 Handbook, Management of Breaches Involving Sensitive Personal Information, as appropriate.

(L) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

(M) Steps taken in response to mitigate or prevent a repetition of the incident.

(j) *Training*. (1) All Contractor employees and subcontractor employees requiring access to VA information or VA information systems shall complete the following before being granted access to VA information and its systems:

(i) On an annual basis, successfully complete the VA Privacy and Information Security Awareness and VA Information Security Rules of Behavior training.

(ii) On an annual basis, sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the VA Information Security Rules of Behavior for Organizational Users, relating to access to VA information and information systems.

(iii) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access.

(2) The Contractor shall provide to the Contracting Officer and/or the COR a copy of the training certificates and affirmation that VA Information Security Rules of Behavior for Organizational Users signed by each applicable employee have been completed and submitted within five (5) days of the initiation of the contract and annually thereafter, as required.

(3) Failure to complete the mandatory annual training and acknowledgement of the VA Information Security Rules of Behavior, within the timeframe required, 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 training and documents are complete.

(k) *Subcontract flow down*. The Contractor shall include the substance of this clause, including this paragraph (k), in subcontracts, third-party agreements, and BAAs, of any amount and in which subcontractor employees, third-party servicers/employees, and business associates will perform functions where they will have access to VA information (including VA sensitive information, i.e., sensitive personal information and protected health information), information systems, information technology (IT) or providing and accessing information technology-related contract services, support services, and related resources (see VAAR 802.101 definition of information technology-related contracts).

(End of clause)

C.15 VAAR 852.204-72 PERSONNEL VETTING AND CREDENTIALING (MARCH 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 (https://pdt.nbis.mil/consent).

Positions/Tasks Designated as Non-Sensitive Positions - Tier 1/Low Risk
Not Applicable
Positions/Tasks Designated as Non-Sensitive Positions - Tier 2/Mod Risk
Not Applicable
Positions/Tasks Designated as Non-Sensitive Positions - Tier 4/High Risk
Service Task / Item Number 1.0

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: Not Applicable

Tier 5: Not Applicable

(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.16 VAAR 852.222-71 COMPLIANCE WITH EXECUTIVE ORDER 13899 (DEVIATION)(APR 2025)

(a) The contractor shall comply with Executive Order 13899, Combating Anti-Semitism, pursuant to Title VI of the Civil Rights Act of 1964 (Title VI), 42 U.S.C. 2000d et seq.

(b) The contractor shall timely disclose, in writing, to the Contracting Officer, whenever, in connection with the award, performance, or closeout of this contract or any subcontract thereunder, the Contractor has credible evidence that a principal, employee, agent, or subcontractor of the Contractor has committed a violation under Executive Order 13899, Combatting Anti-Semitism pursuant to the Civil Rights Act of 1964 (Title VI), 42 U.S.C. 2000d et seq.

(c) The contractor shall include the terms and conditions of this clause in every subcontract or purchase order so that these terms will be binding on every subcontractor or vendor.

(End of Clause)

C.17 VAAR 852.232-72 ELECTRONIC SUBMISSION OF PAYMENT REQUESTS (NOV 2018)

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

(1) *Contract financing payment* has the meaning given in FAR 32.001;

(2) *Designated agency* office means the office designated by the purchase order, agreement, or contract to first receive and review invoices. This office can be contractually designated as the receiving entity. This office may be different from the office issuing the payment;

(3) *Electronic form* means an automated system transmitting information electronically according to the accepted electronic data transmission methods and formats identified in paragraph (c) of this clause. Facsimile, email, and scanned documents are not acceptable electronic forms for submission of payment requests;

(4) *Invoice payment* has the meaning given in FAR 32.001; and

(5) *Payment request* means any request for contract financing payment or invoice payment submitted by the contractor under this contract.

(b) *Electronic payment requests.* Except as provided in paragraph (e) of this clause, the contractor shall submit payment requests in electronic form. Purchases paid with a Government-wide commercial purchase card are considered to be an electronic transaction for purposes of this rule, and therefore no additional electronic invoice submission is required.

(c) *Data transmission.* A contractor must ensure that the data transmission method and format are through one of the following:

(1) VA's Electronic Invoice Presentment and Payment System at the current website address provided in the contract.

(2) Any system that conforms to the X12 electronic data interchange (EDI) formats established by the Accredited Standards Center (ASC) and chartered by the American National Standards Institute (ANSI).

(d) *Invoice requirements.* Invoices shall comply with FAR 32.905.

(e) *Exceptions*. If, based on one of the circumstances in this paragraph (e), the Contracting Officer directs that payment requests be made by mail, the Contractor shall submit payment requests by mail through the United States Postal Service to the designated agency office. Submission of payment requests by mail may be required for—

(1) Awards made to foreign vendors for work performed outside the United States;

(2) Classified contracts or purchases when electronic submission and processing of payment requests could compromise the safeguarding of classified or privacy information;

(3) Contracts awarded by contracting officers in the conduct of emergency operations, such as responses to national emergencies;

(4) Solicitations or contracts in which the designated agency office is a VA entity other than the VA Financial Services Center in Austin, Texas; or

(5) Solicitations or contracts in which the VA designated agency office does not have electronic invoicing capability as described above.

(End of Clause)

C.18 VAAR 852.239-70 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES (FEB 2023)

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

Information technology has the same meaning in FAR 2.101 and also *means* Information and Communication Technology (ICT).

Information system security plan means a formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

(b) *Responsibilities*. The Contractor shall be responsible for information system security for all systems connected to a Department of Veterans Affairs (VA) network or operated by the Contractor for VA, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or other system access to VA information that directly supports the mission of VA.Examples of tasks that require security provisions include—

(1) Hosting of VA e-Government sites or other information technology operations;

(2) Acquisition, transmission, or analysis of data owned by VA with significant replacement cost should the contractor's copy be corrupted; and

(3) Access to VA general support systems/major applications at a level beyond that granted the general public, e.g., bypassing a firewall.

(c) *Information system security plan*. The Contractor shall develop, provide, implement, and maintain an Information System Security Plan. VA information systems must have an information system security plan that provides an overview of the security requirements for the system and describes the security controls in place or the plan for meeting those requirements. This plan shall describe the processes and procedures that the Contractor will follow to ensure appropriate security of information system resources developed, processed, or used under this contract. The information system security plan should include implementation status, responsible entities, resources, and estimated completion dates. Information system security plans may also include, but are not limited to, a compiled list of system characteristics, and key security-related documents such as a risk assessment, PIA, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan. The plan shall address the specific contract requirements regarding information systems related support or services included in the contract, to include the performance work statement (PWS) or statement of work (SOW). The Contractor's Information System Security Plan shall comply with applicable Federal Laws that include, but are not limited to, 40 U.S.C. 11331, the Federal Information Security Modernization Act (FISMA) of 2014 and the E-Government Act of 2002. The plan shall meet information system security requirements in accordance with Federal and VA policies and procedures, and as amended during the term of this contract, and include, but are not limited to the following.

(1) OMB Circular A-130, Managing Information as a Strategic Resource;

(2) National Institute of Standards and Technology (NIST) Guidelines; and

(3) VA Directive 6500, VA Cybersecurity Program, and the directives and handbooks in the VA 6500 series related to VA information (including VA sensitive information and sensitive personal information and information systems security and privacy), as well as those set forth in the contract specifications, statement of work, or performance work statement. These include, but are not limited to, VA Handbook 6500.6, Contract Security; and VA Directive and Handbook 0710, Personnel Security and Suitability Program, which establishes VA's procedures, responsibilities, and processes for complying with current Federal law, Executive Orders, policies, regulations, standards and guidance for protecting VA information, information systems (see 802.101, Definitions) security and privacy, and adhering to personnel security requirements when accessing VA information or information systems.

(d) *Submittal of plan*. Within 90 days after contract award, the Contractor shall submit the Information System Security Plan to the Contracting Officer for review and approval.

(e) *Security accreditation*. As required by current VA policy, the Contractor shall submit written proof of information system security accreditation to the Contracting Officer for non-VA owned systems. Such written proof may be furnished either by the Contractor or by a third party. Accreditation shall be in accordance with VA policy available from the Contracting Officer upon request. The Contractor shall submit for acceptance by the Contracting Officer along with this accreditation a final information system security plan, such as a risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. The accreditation and the final information system security plan and the accompanying documents, such as a risk assessment, security test and evaluation, and disaster recovery/continuity of operations plan.

(f) *Annual validation*. On an annual basis, the Contractor shall verify in writing to the Contracting Officer that the Information System Security Plan remains valid.

(g) *Banners*. The Contractor shall ensure that the official VA banners are displayed on all VA systems (both public and private) operated by the Contractor that contain Privacy Act information before allowing anyone access to the system.The Office of Information Technology will make official VA banners available to the Contractor.

(h) *Screening and access*. The Contractor shall screen all personnel requiring privileged access or limited privileged access to systems operated by the Contractor for VA or interconnected to a VA network in accordance with VA Directives and Handbooks referenced in paragraph (c) of this clause.

(i) *Training*. The Contractor shall ensure that its employees performing services under this contract complete VA security awareness training on an annual basis. This includes signing an acknowledgment that they have read, understand, and agree to abide by the VA Information Security Rules of Behavior (VA National Rules of Behavior) as required by 38 U.S.C. 5723; FAR 39.105, Privacy; clause 852.204-71, Information and Information Systems Security, and this clause on an annual basis.

(j) *Government access*. The Contractor shall provide the Government access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. The Contractor shall provide access to enable a program of information system inspection (to include vulnerability testing), investigation and audit (to safeguard against threats and hazards to the integrity, availability and confidentiality of VA data or to the function of information systems operated on behalf of VA), and to preserve evidence of computer crime.

(k) *Notification of termination of employees*. The Contractor shall immediately notify the Contracting Officer when an employee who has access to VA information systems or data terminates employment.

(l) *Subcontractor flow down requirement*. The Contractor shall incorporate and flow down the substance of this clause to all subcontracts that meet the conditions in paragraph (a) of this clause.

(End of clause)

C.19 VAAR 852.239-76 INFORMATION AND COMMUNICATIONS 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: Noted in section B.5 Product Description

(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.20 ARTIFICIAL INTELLIGENCE IN VA CONTRACTS (MAR 2026)

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.

(End of clause)

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION E - SOLICITATION PROVISIONS

E.1 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):

FAR: http://www.acquisition.gov/far/index.html
VA: http://www.va.gov/oal/library/vaar

(End of Provision)

FAR 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	NOV 2025 (DEVIATION)
52.209-2	PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS-REPRESENTATION	NOV 2015
52.209-11	REPRESENTATION BY CORPORATIONS REGARDING DELINQUENT TAX LIABILITY OR A FELONY CONVICTION UNDER ANY FEDERAL LAW	NOV 2025 (DEVIATION)
52.212-1	INSTRUCTIONS TO OFFERORS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES	OCT 2025 (DEVIATION)
52.217-5	EVALUATION OF OPTIONS	NOV 2025 (DEVIATION)

E.2 52.216-1 TYPE OF CONTRACT (DEVIATION NOV 2025)

The Government contemplates award of a Firm-Fixed Price Contract resulting from this solicitation.

(End of Provision)

E.3 52.219-1 SMALL BUSINESS PROGRAM REPRESENTATIONS (DEVIATION NOV 2025)

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

Economically disadvantaged women-owned small business (EDWOSB) concern means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States and who are economically disadvantaged in accordance with 13 CFR part 127, and the concern is certified by SBA or an approved third-party certifier in accordance with 13 CFR 127.300. It automatically qualifies as a women-owned small business concern eligible under the WOSB Program.

Service-disabled veteran-owned small business (SDVOSB) concern means a small business concern—

(1)(i) Not less than 51 percent of which is owned and controlled by one or more service-disabled veterans 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 service-disabled veterans; and

(ii) The management and daily business operations of which are controlled by one or more service-disabled veterans or, in the case of a service-disabled veteran with permanent and severe disability, the spouse or permanent caregiver of such veteran or;

(2) A small business concern eligible under the SDVOSB Program in accordance with 13 CFR part 128 (see subpart 19.14).

(3) *Service-disabled veteran,* as used in this definition, means a veteran, as defined in 38 U.S.C. 101(2), with a disability that is service-connected, as defined in 38 U.S.C. 101(16), and who is registered in the Beneficiary Identification and Records Locator Subsystem, or successor system that is maintained by the Department of Veterans Affairs' Veterans Benefits Administration, as a service-disabled veteran.

Service-disabled veteran-owned small business (SDVOSB) concern eligible under the SDVOSB Program means an SDVOSB concern that—

(1) Effective January 1, 2024, is designated in the System for Award Management (SAM) as certified by the Small Business Administration (SBA) in accordance with 13 CFR 128.300; or

(2) Has represented that it is an SDVOSB concern in SAM and submitted a complete application for certification to SBA on or before December 31, 2023.

Service-disabled veteran-owned small business (SDVOSB) Program means a program that authorizes contracting officers to limit competition, including award on a sole-source basis, to SDVOSB concerns eligible under the SDVOSB Program.

Small business concern—

(1) 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 in 13 CFR part 121 and the size standard in paragraph (b) of this provision.

(2) *Affiliates*, as used in this definition, means business concerns, one of whom directly or indirectly controls or has the power to control the others, or a third party or parties control or have the power to control the others. In determining whether affiliation exists, consideration is given to all appropriate factors including common ownership, common management, and contractual relationships. SBA determines affiliation based on the factors set forth at 13 CFR 121.103.

Small disadvantaged business concern, consistent with 13 CFR 124.1001, 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 concern means a small business concern—

(1) Not less than 51 percent of which is owned 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 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; and

(2) Whose management and daily business operations are controlled by one or more women.

Women-owned small business (WOSB) concern eligible under the WOSB Program (in accordance with 13 CFR part 127) means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States, and the concern is certified by SBA or an approved third-party certifier in accordance with 13 CFR 127.300.

(b)(1) The North American Industry Classification System (NAICS) code for this acquisition is 513210.

(2) The small business size standard is $47,000,000.00.

(3) The small business size standard for a concern that submits an offer, other than on a construction or service acquisition, but proposes to furnish an end item that it did not itself manufacture, process, or produce (*i.e.*, nonmanufacturer), is 500 employees, or 150 employees for information technology value-added resellers under NAICS code 541519, if the acquisition—

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

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

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

(c) *Representations*.

(1) The offeror represents as part of its offer that—

(i) It [ ] is, [ ] is not a small business concern; or

(ii) It [ ] is, [ ] is not a small business joint venture that complies with the requirements of 13 CFR 121.103(h) and 13 CFR 125.8(a) and (b). [The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.]

(2) [*Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.*] The offeror represents that it [ ] is, [ ] is not, a small disadvantaged business concern as defined in 13 CFR 124.1001.

(3) [*Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.*] The offeror represents as part of its offer that it [ ] is, [ ] is not a women-owned small business concern.

(4) *Women-owned small business (WOSB) joint venture eligible under the WOSB Program*. The offeror represents as part of its offer that it [ ] is, [ ] is not a joint venture that complies with the requirements of 13 CFR 127.506(a) through (c). [*The offeror shall enter the name and unique entity identifier of each party to the joint venture:* _____.]

(5) *Economically disadvantaged women-owned small business (EDWOSB) joint venture*. The offeror represents as part of its offer that it [ ] is, [ ] is not a joint venture that complies with the requirements of 13 CFR part 127.506(a) through (c). [*The offeror shall enter the name and unique entity identifier of each party to the joint venture:* _____.]

(6) *Veteran-owned small business concern.* [*Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.*] The offeror represents as part of its offer that it [ ] is, [ ] is not a veteran-owned small business concern.

(7) *SDVOSB concern.* [*Complete only if the offeror represented itself as a veteran-owned small business concern in paragraph (c)(6) of this provision.*] The offeror represents as part of its offer that it [ ] is, [ ] is not an SDVOSB concern.

(8) *SDVOSB joint venture eligible under the SDVOSB Program.* [*Complete only if the offeror represented itself as a SDVOSB concern in paragraph (c)(7) of this provision.*] The offeror represents as part of its offer that it [ ] is, [ ] is not a SDVOSB joint venture eligible under the SDVOSB Program that complies with the requirements of 13 CFR 128.402. [*The offeror shall enter the name and unique entity identifier of each party to the joint venture:__*.]

(9) *HUBZone small business concern.* [*Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.*] The offeror represents, as part of its offer, that—

(i) It [ ] is, [ ] is not a HUBZone small business concern listed, on the date of this representation, as having been certified by SBA as a HUBZone small business concern in the Dynamic Small Business Search and SAM, and will attempt to maintain an employment rate of HUBZone residents of 35 percent of its employees during performance of a HUBZone contract (see 13 CFR 126.200(e)(1)); and

(ii) It [ ] is, [ ] is not a HUBZone joint venture that complies with the requirements of 13 CFR Part 126.616(a) through (c). [The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.] Each HUBZone small business concern participating in the HUBZone joint venture shall provide representation of its HUBZone status.

(d) *Notice*.

Under 15 U.S.C. 645(d), any person who misrepresents a firm's status as a business concern that is small, HUBZone small, small disadvantaged, service-disabled veteran-owned small, economically disadvantaged women-owned small, or women-owned small eligible under the WOSB Program in order to obtain a contract to be awarded under the preference programs established pursuant to section 8, 9, 15, 31, and 36 of the Small Business Act or any other provision of Federal law that specifically references section 8(d) for a definition of program eligibility, shall—

(1) Be punished by imposition of fine, imprisonment, or both;

(2) Be subject to administrative remedies, including suspension and debarment; and

(3) Be ineligible for participation in programs conducted under the authority of the Act.

(End of Provision)

E.4 52.229-11 TAX ON CERTAIN FOREIGN PROCUREMENTS—NOTICE AND REPRESENTATION (DEVIATION NOV 2025)

(a) Definitions. As used in this provision—

Foreign person means any person other than a United States person.

Specified Federal procurement payment means any payment made pursuant to a contract with a foreign contracting party that is for goods, manufactured or produced, or services provided in a foreign country that is not a party to an international procurement agreement with the United States. For purposes of the prior sentence, a foreign country does not include an outlying area.

United States person as defined in 26 U.S.C. 7701(a)(30) means—

(1) A citizen or resident of the United States;

(2) A domestic partnership;

(3) A domestic corporation;

(4) Any estate (other than a foreign estate, within the meaning of 26 U.S.C. 701(a)(31)); and

(5) Any trust if—

(i) A court within the United States is able to exercise primary supervision over the administration of the trust; and

(ii) One or more United States persons have the authority to control all substantial decisions of the trust.

(b) Unless exempted, there is a 2 percent tax of the amount of a specified Federal procurement payment on any foreign person receiving such payment. See 26 U.S.C. 5000C and its implementing regulations at 26 CFR 1.5000C-1 through 1.5000C-7.

(c) Exemptions from withholding under this provision are described at 26 CFR 1.5000C-1(d)(5) through (7). The Offeror would claim an exemption from the withholding by using the Department of the Treasury Internal Revenue Service Form W-14, Certificate of Foreign Contracting Party Receiving Federal Procurement Payments, available via the internet at *www.irs.gov/w14*. Any exemption claimed and self-certified on the IRS Form W-14 is subject to audit by the IRS. Any disputes regarding the imposition and collection of the 26 U.S.C. 5000C tax are adjudicated by the IRS as the 26 U.S.C. 5000C tax is a tax matter, not a contract issue. The IRS Form W-14 is provided to the acquiring agency rather than to the IRS.

(d) For purposes of withholding under 26 U.S.C. 5000C, the Offeror represents that—

(1) It [ ] is [ ] is not a foreign person; and

(2) If the Offeror indicates "is" in paragraph (d)(1) of this provision, then the Offeror represents that—I am claiming on the IRS Form W-14 [ ] a full exemption, or [ ] partial or no exemption [*Offeror shall select one*] from the excise tax.

(e) If the Offeror represents it is a foreign person in paragraph (d)(1) of this provision, then—

(1) The clause at FAR 52.229-12, Tax on Certain Foreign Procurements, will be included in any resulting contract; and

(2) The Offeror shall submit with its offer the IRS Form W-14. If the IRS Form W-14 is not submitted with the offer, exemptions will not be applied to any resulting contract and the Government will withhold a full 2 percent of each payment.

(f) If the Offeror selects "is" in paragraph (d)(1) and "partial or no exemption" in paragraph (d)(2) of this provision, the Offeror will be subject to withholding in accordance with the clause at FAR 52.229-12, Tax on Certain Foreign Procurements, in any resulting contract.

(g) A taxpayer may, for a fee, seek advice from the Internal Revenue Service (IRS) as to the proper tax treatment of a transaction. This is called a private letter ruling. Also, the IRS may publish a revenue ruling, which is an official interpretation by the IRS of the Internal Revenue Code, related statutes, tax treaties, and regulations. A revenue ruling is the conclusion of the IRS on how the law is applied to a specific set of facts. For questions relating to the interpretation of the IRS regulations go to *https://www.irs.gov/help/tax-law-questions*.

(End of Provision)

E.5 52.233-2 SERVICE OF PROTEST (DEVIATION NOV 2025)

Protests, as defined in section 33.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), shall be served on the Contracting Officer (addressed as follows) by obtaining written and dated acknowledgment of receipt from:

Michael Weckesser

michael.weckesser@va.gov
Hand-Carried Address:

Department of Veterans Affairs

Technology Acquisition Center
Attn: Michael Weckesser
23 Christopher Way
Eatontown NJ 07724
Mailing Address:

Department of Veterans Affairs

Technology Acquisition Center
Attn: Michael Weckesser
23 Christopher Way
Eatontown NJ 07724

(b) The copy of any protest shall be received in the office designated above within one day of filing a protest with the GAO.

(End of Provision)

E.6 52.240-90 SECURITY PROHIBITIONS AND EXCLUSIONS REPRESENTATIONS AND CERTIFICATIONS (DEVIATION NOV 2025)

(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.7 VAAR 852.233-70 PROTEST CONTENT/ALTERNATIVE DISPUTE RESOLUTION (OCT 2018)

(a) Any protest filed by an interested party shall—

(1) Include the name, address, fax number, email and telephone number of the protester;

(2) Identify the solicitation and/or contract number;

(3) Include an original signed by the protester or the protester's representative and at least one copy;

(4) Set forth a detailed statement of the legal and factual grounds of the protest, including a description of resulting prejudice to the protester, and provide copies of relevant documents;

(5) Specifically request a ruling of the individual upon whom the protest is served;

(6) State the form of relief requested; and

(7) Provide all information establishing the timeliness of the protest.

(b) Failure to comply with the above may result in dismissal of the protest without further consideration.

(c) Bidders/offerors and Contracting Officers are encouraged to use alternative dispute resolution (ADR) procedures to resolve protests at any stage in the protest process. If ADR is used, the Department of Veterans Affairs will not furnish any documentation in an ADR proceeding beyond what is allowed by the Federal Acquisition Regulation.

(End of Provision)

E.8 VAAR 852.233-71 ALTERNATE PROTEST PROCEDURE (OCT 2018)

(a) As an alternative to filing a protest with the Contracting Officer, an interested party may file a protest by mail or electronically with: Executive Director, Office of Acquisition and Logistics, Risk Management and Compliance Service (003A2C), Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420 or Email: *EDProtests@va.gov.*

(b) The protest will not be considered if the interested party has a protest on the same or similar issue(s) pending with the Contracting Officer.

(End of Provision)

E.9 VAAR 852.239-71 INFORMATION SYSTEM SECURITY PLAN AND ACCREDITATION (FEB 2023)

All offers submitted in response to this solicitation or request for quotation shall address the approach for completing the security plan and accreditation requirements in clause 852.239–70, Security Requirements for Information Technology Resources.

(End of Provision)

E.10 VAAR 852.239-75 INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY NOTICE (FEB 2023)

(a) Any offeror responding to this solicitation must comply with established VA Information and Communication Technology (ICT) (formerly Electronic and Information (EIT)) accessibility standards. Information about Section 508 is available at *http://www.section508.va.gov/*.

(b) The Section 508 accessibility standards applicable to this solicitation are stated in the clause at 852.239–75, Information and Communication Technology Accessibility. In order to facilitate the Government's determination whether proposed ICT supplies meet applicable Section 508 accessibility standards, offerors must submit appropriate VA Section 508 Checklists, in accordance with the checklist completion instructions. The purpose of the checklists is to assist VA acquisition and program officials in determining whether proposed ICT supplies, or information, documentation and services conform to applicable Section 508 accessibility standards. The checklists allow offerors or developers to self-evaluate their supplies and document—in detail—whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues.

(c) Respondents to this solicitation must identify any exception to Section 508 requirements. If an offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies or services delivered do not conform to the described accessibility standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

(End of Provision)

E.11 ARTIFICIAL INTELLIGENCE EFFORTS (MAR 2026)

Response Instructions: 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, 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: _____

(End of provision)

E.11 BASIS FOR AWARD

Award will be made on a sole source basis as supported by the approved Justification for Other Than Full and Open Competition attached to the posting for this effort upon verification that the quote conforms to the requirements of the solicitation set forth in Section B.4 Price Schedule, and Section B.5 Product Description. Any proposals/quotes that are received shall be evaluated, but any Offeror must submit its quotation on an "All or None" basis. The Government will evaluate offers to ensure conformance with the requirements of the solicitation and by adding the total price for all items to include the Option Periods in the Price Schedule. The total evaluated price will be that sum.

E.12 QUOTE SUBMISSION INSTRUCTIONS

The offeror's quote shall be submitted via email to Michelle Policari (Michelle.Policari@va.gov) and Michael Weckesser (Michael.Weckesser@va.gov). Your response must be received by the closing date indicated on Blocks 6 and 8 of the SF1449, to be considered timely for award of an Order. Please note that file size is limited to 5 mb. **The use of hyperlinks or embedded attachments in quotes is prohibited. Accordingly, any information contained within an embedded attachments and/or hyperlink will neither be accessed nor evaluated.**

The quote shall be submitted in accordance with FAR 52.212-1 as supplemented by the below:

1. Offerors shall complete Section B.4 Price Schedule with the prices for all items in the solicitation.

2. Offerors must meet all the requirements listed in Section B.4 Price Schedule and Section B.5 Product Description and have each requirement outlined in their quote, to include a description of the items being offered in sufficient detail to evaluate conformance with the requirements in the RFQ. No assumptions of compatibility will be made on the part of VA. Failure to list all requirements in their entirety in an Offeror's quote will result in a noncompliant quote.

3. Offerors must submit a quote on an "all or none" basis. Offerors are required to complete/furnish all required information with its quote, which includes, but is not limited

to completion/signature of any required assertion or submission. All offerors are cautioned that any deviation from the Government's minimum terms and conditions set forth in this Solicitation may result in your offer being deemed by the Government to be non-conforming to the requirements and excluded from consideration for award. Accordingly, 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 quote Unacceptable, and thus ineligible for award. This may include, but is not limited to, quotes predicated on incorporation of commercial software license agreements.

4. 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. Examples include paragraph (d) of 52.212-3, Offeror Representations and Certifications—Commercial Products and Commercial Services. 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.

5. Any resulting contract will be awarded on a firm-fixed-price basis as defined by Federal Acquisition Regulation Subpart 16.202. Accordingly, the Offeror shall ensure that any and all costs associated with the Offeror's proposed application(s), software products, software solution, and/or system, shall be included in the Offeror's proposed firm-fixed price, and shall serve as the Offeror's firm-fixed price for the life of any resulting contract. No additional costs or fees relative to the Offeror'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 Offeror's proposed solution will be allowed, accepted, and/or paid by the Government.