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: 36C10B26Q0632

6. SOLICITATION ISSUE DATE: 08-03-2026

7. FOR SOLICITATION INFORMATION CALL:

a. NAME: Ryan Sehulster

b. TELEPHONE NO. (No Collect Calls): 848-377-5190

8. OFFER DUE DATE/LOCAL TIME: 08-10-2026 3:00PM EST

9. ISSUED BY — CODE 36C10B

Department of Veterans Affairs
Technology Acquisition Center

23 Christopher Way
Eatontown NJ 07724

10. THIS ACQUISITION IS

- [ ] UNRESTRICTED OR
- [X] SET ASIDE: 100 % FOR:
- [X] 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: 541519

SIZE STANDARD: $34 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 Delivery Schedule

16. ADMINISTERED BY — CODE 36C10B

Department of Veterans Affairs
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 36C10A

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

PHONE: — 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	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Title: Data Engineering, Management Support and Quality Assurance Recommendations Contracting Officer: Kimberly Geran, Kimberly.Geran@va.gov Contract Specialist: Ryan Sehulster, Ryan.Sehulster@va.gov Purchase Order Number: TBD (Use Reverse and/or Attach Additional Sheets as Necessary)				

25. ACCOUNTING AND APPROPRIATION DATA

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

- [ ] 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) — 31c. DATE SIGNED

Table of Contents

SECTION A 1

A.1 SF 1449 SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES 1
A.2 COMBINED SYNOPSIS/SOLICITATION 3
A.3 GOVERNING LAW 3
A.4 SOFTWARE LICENSE, SOFTWARE MAINTENANCE AND SOFTWARE TECHNICAL SUPPORT: 4
A.5 CONTRACT ADMINISTRATION DATA 9

SECTION B 10

B.1 PRICE SCHEDULE 10
B.2 PERFORMANCE WORK STATEMENT 18

SECTION C - CONTRACT CLAUSES 77

C.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998) 77
C.2 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000) 79
C.3 52.240-93 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (DEVIATION) (NOV 2025) 79
C.4 VAAR 852.239-76 INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY (FEB 2023) 81

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS 83

SECTION E - SOLICITATION PROVISIONS 84

E.1 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998) 84
E.2 52.209-7 INFORMATION REGARDING RESPONSIBILITY MATTERS (NOV 2025) (DEVIATION) 84
E.3 52.216-1 TYPE OF CONTRACT (NOV 2025) (DEVIATION) 86
E.4 52.233-2 SERVICE OF PROTEST (SEP 2006) 86
E.5 BASIS FOR AWARD 86
E.6 SUBMISSION INSTRUCTIONS 89

A.2 COMBINED SYNOPSIS/SOLICITATION

This is a combined synopsis/solicitation for commercial products or commercial services prepared in accordance with part 12. This announcement constitutes the only solicitation. Offers are being requested and a separate written solicitation will not be issued.

(i) Solicitation number 36C10B26Q0632 is issued as a Request for Quotation (RFQ) 36C10B26Q0632 for Data Engineering, Management Support and Quality Assurance Recommendations.

This acquisition is ~~not~~ set-aside for small business concerns. This solicitation incorporates provisions and clauses by reference. The full text of provisions and clauses may be accessed electronically at www.acquisition.gov.

(ii) See Section B below for the Schedule of Deliverables.

(iii) See Section B below for the Performance Work Statement.

(iv) See Section B below for the Delivery/Acceptance/F.O.B.

(v) See Section E below for the Provisions.

(vi) See Section C below for the Clauses.

(vii) Offers are due by 3PM EST on August 10, 2026. Offerors shall submit quotes via email to Ryan.Sehulster@va.gov.

(viii) Please contact Contract Specialist, Ryan Sehulster, Ryan.Sehulster@va.gov, (848) 377-5190, or Contracting Officer, Kimberly Geran, Kimberly.Geran@va.gov, (848) 377-5228 for information regarding the solicitation.

A.3 GOVERNING LAW

Federal law and regulations, including the Federal Acquisition Regulations (FAR), shall govern this Contract/Order. Commercial license agreements may be made a part of this Contract/Order but only if both parties expressly make them an addendum hereto. If the commercial license agreement is not made an addendum, it shall not apply, govern, be a part of or have any effect whatsoever on the Contract/Order; this includes, but is not limited to, any agreement embedded in the computer software (clickwrap), any agreement that is otherwise delivered with or provided to the Government with the commercial computer software or documentation (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 clauses and the provisions of this Contract/Order; those provisions in the commercial license agreement that do not address data rights regarding the Government's use, duplication and disclosure of data shall not be included or made a part of the Contract/Order. Federal law and regulation including,

without limitation, the Contract Disputes Act (41 U.S.C. § 7101 et seq.), the Anti-Deficiency Act (31 U.S.C. § 1341 et seq.), the Competition in Contracting Act (41 U.S.C. § 3301 et seq.), the Prompt Payment Act (31 U.S.C. § 3901 et seq.), Contracts for Data Processing or Maintenance (38 USC § 5725), Source Code Harmonization and Reuse in Information Technology Act "SHARE IT Act" (P.L. 118-187), and FAR clauses 52.212-4, 52.227-14 shall supersede, control, and render ineffective any inconsistent, conflicting, or duplicative provision in any commercial license agreement. In the event of conflict between this clause and any provision in the Contract/Order or the commercial license agreement or elsewhere, the terms of this clause shall prevail. The Contractor shall deliver to the Government all data first produced under this Contract/Order with unlimited rights as defined by FAR 52.227-14, this includes any custom code developed for the purpose of performing under this contract. Claims of patent or copyright infringement brought against the Government as a party shall be defended by the U.S. Department of Justice (DOJ) in accordance with 28 U.S.C. § 516; at the discretion of DOJ, the Contractor may be allowed reasonable participation in the defense of the litigation. Any additional changes to the Contract/Order must be made by modification (Standard Form 30) and shall only be made by a warranted Contracting Officer. Nothing in this Contract/Order or any commercial license agreement shall be construed as a waiver of sovereign immunity.

A.4 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 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.

A.5 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, Kimberly Geran
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] See B.1 Price Schedule

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

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

AMENDMENT NO	DATE

SECTION B

B.1 PRICE SCHEDULE

NOTE: Vendors are instructed to complete Section B.1 and submit with their quote.

Vendors are cautioned that alterations to the line items as specified below may render quotes unacceptable. All questions shall be directed to the Contract Specialist, Ryan Sehulster, Ryan.Sehulster@va.gov and Contracting Officer, Kimberly.Geran@ga.gov prior to the closing date and time specified in the Request for Proposals (RFP).

Base Period **The Period of Performance (PoP) shall be 12 months from date of Award.**					
CLIN	**Description**	**Qty**	**Unit**	**Unit Price**	**Extended Price**
0001	**Project Management** shall be provided in accordance with (IAW) Performance Work Statement (PWS) paragraph 5.1. This Firm-Fixed Price (FFP) Contract Line-Item Number (CLIN) includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.1 inclusive of all of its subparagraphs.	12	MO	$	$
0001AA	**Monthly Contractor Project Management** Plan IAW PWS paragraph 5.1. These reports shall reflect data as of the last day of the preceding month. Timeline to be determined during transition. Electronic submission to: VA PM, COR Inspection: Destination Acceptance: Destination	1	LT	NSP	NSP
0001AB	**Monthly Progress Report** IAW PWS paragraph 5.1.2. These reports shall reflect data as of the last day of the preceding	1	LT	NSP	NSP

	month. Timeline to be determined during transition. Electronic submission to: VA PM, COR Inspection: Destination Acceptance: Destination				
0002	**Data Engineering, Management Support, and Quality Assurance Recommendations** IAW PWS paragraph 5.2. This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.2 inclusive of all of its subparagraphs.	12	MO	$	$
0002AA	**Grant Manager Review and Monitor Process** IAW PWS paragraph 5.2. Due Date will be provided at time of award. Electronic submission to: VA PM, COR Inspection: Destination Acceptance: Destination	1	LT	NSP	NSP
0002AB	**Suicide Prevention Plan** IAW PWS paragraph 5.2. Due Date will be provided at time of award. Electronic submission to: VA PM, COR Inspection: Destination Acceptance: Destination	1	LT	NSP	NSP
0002AC	**Analyze Data, Compiled Briefings and Reports** IAW PWS paragraph 5.2	1	LT	NSP	NSP

	Due Date will be provided at time of award. Electronic submission to: VA PM, COR Inspection: Destination Acceptance: Destination				
0002AD	**Data Collection Tool Documentation of New Requirements** IAW PWS paragraph 5.2 Due Date will be provided at time of award. Electronic submission to: VA PM, COR Inspection: Destination Acceptance: Destination	1	LT	NSP	NSP
				Base Period Total:	**$**

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 period shall commence immediately after expiration of the Base Period.

Period of Performance shall be 12 months from the expiration of the Base Period.

CLIN	Description	Qty	Unit	Unit Price	Extended Price
1001	**Project Management** shall be provided in accordance with (IAW) Performance Work Statement (PWS) paragraph 5.1. This Firm-Fixed Price (FFP) Contract Line-Item Number (CLIN) includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.1 inclusive of all of its subparagraphs.	12	MO	$	$

1001AA	**Monthly Contractor Project Management Plan** IAW PWS paragraph 5.1.1. These reports shall reflect data as of the last day of the preceding month. Timeline to be determined during transition. Electronic submission to: VA PM, COR Inspection: Destination Acceptance: Destination	1	LT	NSP	NSP
1001AB	**Monthly Progress Report** IAW PWS paragraph 5.1.2 These reports shall reflect data as of the last day of the preceding month. Timeline to be determined during transition. Electronic submission to: VA PM, COR Inspection: Destination Acceptance: Destination	1	LT	NSP	NSP
1002	**Data Engineering, Management Support, and Quality Assurance Recommendations** IAW PWS paragraph 5.2. This Firm-Fixed Price (FFP) Contract Line-Item Number (CLIN) includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.2 inclusive of all of its subparagraphs.	12	MO	$	$
1002AA	**Grant Manager Review and Monitor Process** IAW PWS paragraph 5.2. Due Date will be provided at time of award.	1	LT	NSP	NSP

	Electronic submission to: VA PM, COR Inspection: Destination Acceptance: Destination				
1002AB	**Suicide Prevention Plan** IAW PWS paragraph 5.2. Due Date will be provided at time of award. Electronic submission to: VA PM, COR Inspection: Destination Acceptance: Destination	1	LT	NSP	NSP
1002AC	**Analyze Data, Compiled Briefings and Reports** IAW PWS paragraph 5.2. Due Date will be provided at time of award. Electronic submission to: VA PM, COR Inspection: Destination Acceptance: Destination	1	LT	NSP	NSP
1002AD	**Data Collection Tool Documentation of New Requirements** IAW PWS paragraph 5.2. Due Date will be provided at time of award. Electronic submission to: VA PM, COR Inspection: Destination Acceptance: Destination	1	LT	NSP	NSP
				Option Period 1 Total:	**$**
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 period shall commence immediately after expiration of Option Period One.					

Period of Performance shall be 12 months from the expiration of Option Period 1.					
CLIN	**Description**	**Qty**	**Unit**	**Unit Price**	**Extended Price**
2001	**Project Management** shall be provided in accordance with (IAW) Performance Work Statement (PWS) paragraph 5.1. This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.1 inclusive of all of its subparagraphs.	12	MO	$	$
2001AA	**Monthly Contractor Project Management Plan** IAW PWS paragraph 5.1.1. These reports shall reflect data as of the last day of the preceding month. Timeline to be determined during transition. Electronic submission to: VA PM, COR Inspection: Destination Acceptance: Destination	1	LT	NSP	NSP
2001AB	**Monthly Progress Report** IAW PWS paragraph 5.1.2. These reports shall reflect data as of the last day of the preceding month. Timeline to be determined during transition. Electronic submission to: VA PM, COR Inspection: Destination Acceptance: Destination	1	LT	NSP	NSP
2002	**Data Engineering, Management Support, and Quality Assurance Recommendations** IAW PWS paragraph 5.2	12	MO	$	$

	This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.2 inclusive of all of its subparagraphs.				
2002AA	**Grant Manager Review and Monitor Process** IAW PWS paragraph 5.2. Due Date will be provided at time of award. Electronic submission to: VA PM, COR Inspection: Destination Acceptance: Destination	1	LT	NSP	NSP
2002AB	**Suicide Prevention Plan** IAW PWS paragraph 5.2 Due Date will be provided at time of award. Electronic submission to: VA PM, COR Inspection: destination Acceptance: destination	1	LT	NSP	NSP
2002AC	**Analyze Data, Compiled Briefings and Reports** IAW PWS paragraph 5.2. Due Date will be provided at time of award. Electronic submission to: VA PM, COR Inspection: Destination Acceptance: Destination	1	LT	NSP	NSP
2002AD	**Data Collection Tool Documentation of New Requirements** IAW PWS paragraph 5.2.	1	LT	NSP	NSP

	Due Date will be provided at time of award. Electronic submission to: VA PM, COR Inspection: Destination Acceptance: Destination				
				Option Period 2 Total:	**$**
				Grand Total (Base + Option Periods 1 + 2):	**$**

B.2 PERFORMANCE WORK STATEMENT

PERFORMANCE WORK STATEMENT

DEPARTMENT OF VETERANS AFFAIRS

Veterans Health Administration (VHA)
Office of Mental Health and Suicide Prevention

Data Engineering, Management Support and Quality Assurance Recommendations

Date: July 23, 2026
PWS Version Number: 2.0

1.0 BACKGROUND

The Department of Veterans Affairs (VA), Veterans Health Administration (VHA) Office of Mental Health and Suicide Prevention, strives to reduce military and Veteran suicide by focusing on clinical interventions and community-based outreach prevention strategies. Through this program, VA has offered grants to eligible entities, identified in the regulations, for providing or coordinating suicide prevention services to Veterans and their families. The goal of the program is to identify Veterans who are at risk of suicide and their family members and to provide them with suicide prevention services either through VA or the community.

The SSG Fox Suicide Prevention Grant Program (SPGP) is authorized pursuant to the Commander John Scott Hannon Veterans Mental Health Care Improvement Act of 2019 (Public Law 116-171) and implemented by final rule, promulgating 38 C.F.R. part 78. Per 38 C.F.R. part 78, grantees may provide the following suicide prevention services to program participants: Outreach to identify those at risk of suicide; Baseline mental health screening to eligible individuals; Education of communities, Veterans and families on suicide risk and prevention, how to identify those at risk of suicide, how and when to make referrals for care, and the types of suicide prevention resources available within the area; Provision of clinical services for emergency treatment; Case management services; Peer support services; VA benefits assistance for eligible individuals and their families; Assistance with obtaining and coordinating other benefits provided by the federal VA, a state or local VA, or an eligible entity; Assistance with emergent needs relating to health care services, daily living services, personal financial planning and counseling, transportation services, temporary income support services, fiduciary and representative payee services, legal services to assist the eligible individual with issues that may contribute to the risk of suicide, and child care. In addition, grantees may provide nontraditional and innovative approaches and treatment practices, as determined appropriate by VA.

In November 2021, VA engaged the MITRE Federally Funded Research Development Centers (FFRDC) to perform an Analysis of Alternatives (AoA) for a functional prototype for data collection tools and processes for grantees for the SSG Fox SPGP. The FFRDC was required to explore the potential use of up to five existing applications in use at VA and deliver an AoA with findings, risks, and an overall recommendation. That analysis was delivered to VA and as a result the VA OSP selected the existing VA Behavioral Health Lab (BHL) Touch platform as the application to be configured for the SSG Fox SPGP. The BHL Platform collects several of the same data within the VA by Veterans Health Administration (VHA) providers as was needed to collect from the grantees (not directly affiliated with VA) for the suicide prevention grant program.

MITRE conducted the BHL Touch system configuration to allow for additional data collection via BHL interview forms to comply with Congressional statute for a data collection tool. The Data Collection Tool (DCT) operates in VA's Enterprise Cloud environment (VAEC) and achieved an Authority to Operate in June of 2025 for another two (2)-year period. From 2022 through 2024, VA continued to refine the DCT, identifying and testing additional data collection needs to meet statute requirements. The DCT functional prototype allowed VA to demonstrate the ability to securely collect

sensitive de-identified Veteran mental health/suicide risk data which by law has been included in the Interim Congressionally Mandated Report (CMR) and is in process of being included in the Final CMR. VA demonstrated the success of the functional prototype and is now able to continue operation of the DCT in their production environment which will allow the program to engage additional grantees to the program for 2026 and beyond. The DCT platform is now undergoing transition back to VA or to another expected contractor to continue to manage the DCT environment which is mandated by the statute.

SSG Fox SPGP has entered its fourth year. VA published the Notice of Funding Opportunity (NOFO) for Fiscal Year (FY) 2026 SSG Fox SPGP services on May 15, 2025. The NOFO assumes that Congress will extend the authority beyond September 2025 and appropriate funds consistent with section 201 of the Hannon Act as currently written. Applications are due July 18, 2025, and the awards will be announced by September 30, 2025. OSP allocated approximately $52M to avoid a disruption in services through this NOFO, and Congress finalized legislative extension and appropriations as anticipated, another NOFO could soon follow.

2.0 APPLICABLE DOCUMENTS

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

1. “Federal Information Security Modernization Act of 2014.”
2. Federal Information Processing Standards (FIPS) Publication 140-3, “Security Requirements for Cryptographic Modules”, March 22, 2019
3. Federal Information Processing Standard (FIPS) Publication 140-2, “Security Requirements for Cryptographic Modules.”
4. FIPS Pub 199. “Standards for Security Categorization of Federal Information and Information Systems,” February 2004.
5. FIPS Pub 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006.
6. FIPS Pub 201-3, “Personal Identity Verification of Federal Employees and Contractors,” January 2022.
7. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974.”
8. Public Law 109-461 (P.L. 109-461), Veterans Benefits, Health Care, and Information Technology Act of 2006, as amended, Title IX, Information Security Matters.
9. 42 U.S.C. § 2000d “Title VI of the Civil Rights Act of 1964”, as amended.
10. VA Directive 0710, “Personnel Security and Suitability Program,” June 4, 2024, https://www.va.gov/vapubs/index.cfm.
11. VA Handbook 0710, “Personnel Security and Suitability Program,” May 2, 2016, https://www.va.gov/vapubs/index.cfm.
12. 36 C.F.R. Part 1194 “Information and Communication Technology Standards and Guidelines,” as amended.
13. Office of Management and Budget (OMB) Circular A-130, “Managing Federal Information as a Strategic Resource,” July 28, 2016.

14. NIST SP 800-66 Rev. 2, “Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide,” February 2024.
15. 45 C.F.R Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”); and 45 C.F.R. Parts 160 and 164, Subparts A and C, the Security Standard (“Security Rule”); as amended.
16. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended, January 18, 2017.
17. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004.
18. VA Handbook 6500.6, “Contract Security,” March 12, 2010 (see VA Notice 24-12, dated April 22, 2024, “Update to VA Handbook 6500.6, Contract Security, Appendix C VA Information and Information System Security/Privacy Language For Inclusion Into Contracts, As Appropriate”).
19. OIT Process Asset Library (PAL), OIT Process Asset Library. Reference Process Maps at https://www.va.gov/process/maps.asp and Artifact templates at https://www.va.gov/process/artifacts.asp.
20. One-VA Technical Reference Model (TRM) (reference at https://www.va.gov/trm/TRMHomePage.aspx).
21. VA Directive 6508, “Implementation of Privacy Threshold Analysis and Privacy Impact Assessment,” October 15, 2014.
22. VA Handbook 6510, “VA Identity, Credential and Access Management,” September 27, 2024.
23. VA Directive and Handbook 6513, “Secure External Connections,” October 12, 2017.
24. VA Directive 6300, “Records and Information Management,” September 21, 2018.
25. VA Handbook, 6300.1, “Records Management Procedures, “March 24, 2010.
26. NIST SP 800-37 Rev 2, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,” December 2018.
27. NIST SP 800-53 Rev. 5, “Security and Privacy Controls for Federal Information Systems and Organizations,” September 23, 2020 (includes updates as of 12/10/2020).
28. VA Directive 0735, “Homeland Security Presidential Directive 12 (HSPD-12) Program,” October 26, 2015.
29. OMB Memorandum 05-24, “Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors,” August 5, 2005.
30. OMB Memorandum M-19-17, “Enabling Mission Delivery Through Improved Identity, Credential, and Access Management,” May 21, 2019.
31. OMB Memorandum, “Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation,” May 23, 2008.
32. Federal Identity, Credential, and Access Management (FICAM) Architecture, June 30, 2023 (FICAM Architecture (idmanagement.gov)).
33. NIST SP 800-116 Rev 1, “Guidelines for the Use of Personal Identity Verification (PIV) Credentials in Facility Access,“ June 2018.

34. NIST SP 800-63-3, 800-63A, 800-63B, 800-63C, “Digital Identity Guidelines,” updated March 02, 2020.
35. NIST SP 800-157, “Guidelines for Derived PIV Credentials,” December 2014.
36. VA Memorandum, VAIQ #7100147, “Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12),” April 29, 2011 (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514).
37. Identity Access Management (IAM) Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, Personal Identity Verification (PIV)/IAM (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514).
38. VA Memorandum “Personal Identity Verification (PIV) Logical Access Policy Clarification,” July 17, 2019, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4896.
39. Trusted Internet Connections (TIC) 3.0 Core Guidance Documents, https://www.cisa.gov/publication/tic-30-core-guidance-documents.
40. OMB Memorandum M-19-26, “Update to the Trusted Internet Connections (TIC) Initiative,” September 12, 2019.
41. OMB Memorandum M-08-23, “Securing the Federal Government’s Domain Name System Infrastructure,” August 22, 2008.
42. Office of Information Security (OIS) VAIQ #7424808 Memorandum, “Remote Access,” January 15, 2014, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28.
43. VA Memorandum “Proper Use of Email and Other Messaging Services,” January 2, 2018, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28.
44. Social Security Number (SSN) Fraud Prevention Act of 2017.
45. NIST SP 800-52 Revision 2, “Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations.
46. OMB M-22-18, “Enhancing the Security of the Software Supply Chain through Secure Software Development Practices,” September 14, 2022.
47. OMB M-23-16, “Update to Memorandum M-22-18,” June 9, 2023.
48. CISA Binding Operational Directive (BOD) 19-02: “Vulnerability Remediation Requirements of Internet-Accessible Systems,” April 29, 2019, BOD 19-02: Vulnerability Remediation Requirements for Internet-Accessible Systems | CISA.
49. CISA BOD 22-01: “Reducing the Significant Risk of Known Exploited Vulnerabilities,” November 3, 2021, BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities | CISA.
50. CISA BOD 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks.” Cybersecurity & Infrastructure Security Agency (CISA), BOD 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks | CISA.
51. VA Memorandum, “VA Security Controls,” January 17, 2025, https://www.voa.va.gov/DocumentView.aspx?DocumentID=5010.
52. SSG Fox SPGP Website for the current list of grantees here: https://www.mentalhealth.va.gov/ssgfox-grants/index.asp.

3.0 SCOPE OF WORK

The Contractor shall support VA with the operation of the DCT, as well as the processes for grantees to review data quality. Furthermore, the Contractor shall provide the DCT Data Engineering, Management Support, and Quality Assurance Recommendations and complete the specific task and deliverables set forth in Section 5.0 below.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The Period of Performance (PoP) shall be a 12-month base period, with two, 12-month option periods.

Any work at the Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO).

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

Under current definitions, five are set by date:

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

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

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

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

4.2 PLACE OF PERFORMANCE

Tasks under this PWS shall be performed primarily at Contractor facilities. The Contractor shall identify the Contractor’s place of performance in their proposal submission.

In the event that VA requires the Contract to travel to a VA site, any work at a VA site shall not take place on Federal holidays or weekends unless directed by the CO or the Contracting Officer’s Representative (COR).

4.3 TRAVEL

The Government anticipates travel under this effort to perform the tasks associated with the effort. The Contractor shall include all estimated travel costs in firm-fixed-price line items as these costs will not be directly reimbursed by the Government.

There are two (2) in-person conferences per each year of the PoP where the Contractor, VA, and the grantees enrolled in SSG Fox SPGP are required to attend. The location of the travel will not be known until determined by VA during the PoP.

The following is VA's estimated long-distance travel estimate (per year):

Destination	Number of trips	Length of each trip (days)	Number of Contractor Staff traveling per trip
TBD	2	3-5	2

Travel shall be in accordance with the Federal Travel Regulations and requires advanced concurrence by the COR. Contractor travel within the local commuting area will not be reimbursed.

5.0 SPECIFIC TASKS AND DELIVERABLES

5.1 PROJECT MANAGEMENT

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall deliver a Contractor Project Management Plan (CPMP) that lays out the Contractor's approach, timeline, and tools to be used in execution of the contract. The CPMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks, and resource support. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The initial baseline CPMP shall be concurred upon and updated in accordance with Section B of the contract. The Contractor shall update and maintain the VA Program Manager (PM) approved CPMP throughout the PoP.

Deliverable:

A. Monthly Contractor Project Management Plan

5.1.2 REPORTING REQUIREMENTS

The Contractor shall provide the COR with Monthly Progress Reports in electronic form in Microsoft Word and Project formats. The report shall include detailed instructions/explanations for each required data element, to ensure that data is accurate and consistent. These reports shall reflect data as of the last day of the preceding Month.

The Monthly Progress Reports shall cover all work completed during the reporting period and work planned for the subsequent reporting period. The report shall also identify any problems that arose and a description of how the problems were

resolved. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving the issue. The report shall also include an itemized list of all Information and Communication Technology (ICT) deliverables and their current Section 508 conformance status. The Contractor shall monitor performance against the CPMP and report any deviations. It is expected that the Contractor will keep in communication with VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

Deliverable:

A. Monthly Progress Report

5.2 DATA ENGINEERING, MANAGEMENT SUPPORT, AND QUALITY ASSURENCE RECOMMENDATIONS

The Contractor shall collaborate with VA to support the operation of the DCT, as well as the processes for grantees to review data quality. The Contractor shall provide the DCT Data Engineering, Management Support, and Quality Assurance Recommendations.

The Contractor shall receive support for the following activities:

- The Contractor shall receive a knowledge transfer through observation and demonstrating their ability to start and stop the web application and databases, including the onboarding application and extraction, transformation and loading (ETL) process. The ETL process moves the data from VA's Behavioral Health Lab Commercial Off-The-Shelf (COTS) product that was used to configure the DCT to the secure VA Enterprise Cloud which is used to further prepare the data for ingesting into VA's Power Business Intelligence (BI) tool. VA anticipates continued use of the VA's Enterprise License for Microsoft Power BI for the SSG Fox SPGP until such time that VA mandates the use of any other enterprise BI tool.

- The Contractor shall receive a knowledge transfer through observation and demonstrate their ability to control the schedule of this data being moved from one environment to the next in the event of any disruptions in the process.

- The contractor shall receive a knowledge transfer through observation and demonstrating their understanding and comprehension of troubleshooting Technical Assistance logs, where alerts go, and receiving alerts.

- The Contractor shall receive a knowledge transfer through observation and demonstrating their ability to support the transition as the site administrator.

- The Contractor shall track, monitor, and archive data in the DCT from grantees who provide or coordinate suicide prevention services to eligible individuals and their families on the notification (from initial day of enrollment in the grantee or subcontractor program) that the recipients of such services are being paid for, in whole or in part, by the department. The Contractor will not have access to view payment information for grantees. The Contractor shall provide a dashboard that

allows VA to track and monitor the services that are being reported for each participant on a monthly basis which can be viewed from the initial day of enrollment.

- Data shall be archived in several ways:
  - Allowing a grantee to submit through the BHL Touch a request to archive a previous interview's data (e.g., screening, service form, etc.) and submit a new replacement form.
  - Providing a backend process to close out old Adobe records that are not active.
  - Filtering out retiring grantee data (grantee's no longer in the program) from the dashboard views (while still retaining that data in the database)

- The Contractor shall research and coordinate with VA to identify and recommend a process for grant managers to review and monitor compliance using a development plan. The development of the process has begun and each development plan is developed in consultation with the eligible individual and their family. This process will occur outside the DCT, however, the Contractor shall provide guidance for how DCT can be further used in this process.

- The Contractor shall manage data quality assurance protocols for archiving and analyzing data for monthly, quarterly, and annual reports. The data quality assurance protocol shall address data use and transfer security. The Contractor shall analyze data and compile briefings and reports with grantees data on monthly, quarterly, and annual bases for reporting and regular dissemination to VA.

- The Contractor shall create DCT documentation of new requirements as a result of Congressional feedback and program policy changes, coordinate with VA and other vendors in the design of new online data collection forms as a result of policy changes; update the data extract, transformation, and load processes, and prepare the data for ingestion into the data analytics platform.
- The Contractor shall recommend the requirements, design, and testing necessary for reducing the maintenance burdens and costs to VA.

- The Contractor shall include the definitions of the required roles and responsibilities for the data engineering, management support, and quality assurance for the DCT over time.

- The Contractor shall maintain the DCT in the enterprise cloud Authority to Operate (ATO).

- The Contractor shall support VA with the implementation of systems configuration, coordinating with the VA COTS vendor.

Deliverables:

A. Grant Manager Review and Monitor Process

B. Suicide Prevention Plan
C. Analyze Data, Compiled Briefings and Reports
D. DCT Documentation of New Requirements

5.3 SUSTAINMENT SUPPORT CAPABILITIES AND SKILLS

The contractor shall have the following capabilities and skills:

5.3.1 CONFIGURATION MANAGEMENT AND APPLICATION STACK (E.G., DATA ACCESS LAYER, BUSINESS LOGIC) AND DATA MODELS

1. The Contractor shall have experience working with COTS product vendors as well as other contractors responsible for implementing ISO standards, protocols, and other integrative technologies.
2. The Contractor shall have deep systems integration expertise for configuration of a forms-based COTS solution, including systems integration experience and configuring and integrating COTS software via API

5.3.2 CLOUD ENGINEERING

The Contractor shall have experience in systems configuration with an existing COTS product in a Federal Cloud Enterprise, such as VA's Enterprise Cloud, where the solution offers secure access for external-facing users without credentialing, utilizing VA authorized identity providers.

5.3.3 DEVELOPMENT OPERATIONS (DEVOPS)

The Contractor shall have strong software and DevOps implementation expertise and demonstrated experience in implementing solutions that receive and share health information, working within an architecture that segments data to ensure sensitive information is separated from any identifying information.

5.3.4 SYSTEM MONITORING AND TROUBLESHOOTING

The Contractor shall have provision of near-real-time monitoring capabilities for usage patterns and network traffic monitoring.

5.3.5 FEDERAL DATA SECURITY AND PRIVACY REQUIREMENTS IMPLEMENTATION

The Contractor shall have experience achieving and maintaining an ATO for a federally implemented COTS product requiring additional systems configuration, where that product collects sensitive health information that must be protected.

5.3.6 DEVELOPMENT AND MANAGEMENT OF TECHNICAL SYSTEMS DOCUMENTATION

The Contractor shall have provision of well-documented system configuration guides and other technical documentation resources.

5.4 TRANSITION ACTIVITY TIMELINE

The Contractor shall be provided recommendations from MITRE, the current Contractor and the VA, to include but not limited to: staffing with the right engineering and architectural support for the data engineering, management support, and quality assurance activities post-transition from MITRE.

The Contractor shall work with the MITRE over the course of approximately six months using the Data Engineering, Management Support, and Quality Assurance Transition Plan. VA will review the recommendations and determine the appropriate approach to support the transition.

The Contractor shall have roles and responsibilities transitioned from MITRE, on a regular basis.

The Contractor shall perform the following activities:

1. Participate in knowledge sharing and regular meetings to acclimate the data engineer(s)/architect(s) into VA's cloud infrastructure activities as it relates to the DCT:

    a. Vendor coordination between MITRE, VA OSP, and Neuroflow

    b. VAEC Concierge Scrum

    c. Leadership call

    d. Data call

2. Onboard to access resources such as Source Control, VAEC SPGP environment, and cloud devices

3. Learn and comprehend the architecture, integrations, and code

4. Assigned troubleshooting tickets for triage

5. Assigned Development Environment and Pre-Production Environment (PPD) deployment roles

6. Assigned PPD testing and quality assurance (QA) roles

7. Assigned Production Environment deployments and QA checks

At each step, the Contractor shall consult with the COR to ensure timeliness and completion of all tasks.

5.4.1 MONTH 1: IDENTIFYING ROLES AND RESPONSIBILITIES

During the first month of the transition, the Contractor shall have VA badge and be ready to begin working with MITRE in the VAEC.

1. The Contractor shall obtain access to all applicable assistance with the direction of the VA and MITRE after award, including requests for the necessary certifications from MITRE.

2. The Contractor shall be introduced to the following:

    a. The role that the Neuroflow Team plays in providing operational support for the DCT.

    b. The interactions that occur between the Neuroflow Team and MITRE Team, along with VA OSP Program staff.

    c. The processes in place for coordinating across teams when new business requirements are identified or when errors are discovered with the BHL Touch that require coordination.

5.4.2 MONTHS 1–2: GOVERNANCE TRANSITION OVERVIEW

The Contractor shall understand the technical governance activities within the VAEC within the first month of the transition. This includes:

1. Achieving compliance for the 100+ controls

2. Conducting report-outs to the system steward and ISSO

3. Managing key policies and procedures, including:

    a. Managing privileges for user access

    b. Requesting new data pulls from VA's grant management system at the beginning of the new grant award cycle for new grantees, including those that received a renewal, and those that will no longer continue in the program

Other activities that will be included during this first-month transition period related to governance include engaging key stakeholders across VA involved in review and approval of the ATO.

At the end of this period, the Contractor shall:

1. Actively participate in the meetings that regularly take place with the VA OI&T teams.

2. Align staff to the timeline for addressing the ATO roadmap.

3. Achieve access to the VAEC Virtual Private Cloud (VPC) and AWS Console.

4. Obtain and document key contact points at Neuroflow, VA OI&T, MITRE, and VA OSP Program staff.

5.4.3 MONTHS 2–3: VAEC AND THE DCT INFRASTRUCTURE AND DEPLOYMENT OVERVIEW

1. The Contractor shall review and comprehend the architecture design document that was delivered to the VA OSP Program team on March 28, 2024.

2. The Contractor shall obtain access to the Development, Pre-Production, and Production environments. The VA OSP Business Operations Manager must approve access.

3. The Contractor shall identify and own a set of initial tasks.

5.4.4 MONTHS 3–6: TRANSITIONING OPERATIONS AND MAINTENANCE ACTIVITIES

1. The Contractor shall begin integrating into the day-to-day activities for managing the SSG Fox SPGP infrastructure.

2. The Contractor shall review and comprehend the engineering management support that shall be provided to the SSG Fox project through planning, execution, and adoption of any changes to the infrastructure.

3. The Contractor shall understand how to prepare project plans for defining and implementing any new infrastructure updates or specifications. This includes a detailed work breakdown structure that integrates other contractor and vendor activities or dependencies into the plan.

4. The Contractor shall integrate into the ongoing working group meetings to continue to maintain the strong relationships with the VA OSP Program staff, Neuroflow Team, and VA OI&T teams.

5.4.5 MONTHS 3–6: TRANSITIONING NEW REQUIREMENTS AND ENHANCEMENT ACTIVITIES

The Contractor shall work with MITRE and VA OSP Program staff to define and document the detailed requirements for handling participants that complete the program and then later return to the program.

The Contractor Shall:

1. Implement this effort

2. Design and implement any new forms that are needed.

3. Provide the initial mapping of that data for the data pipeline.

5.5 TRANSITIONING OPERATIONS AND MAINTENANCE TASKS

5.5.1 ESTABLISHING AND MANAGING PERMISSIONS/USER ACCESS

The Contractor shall understand the permission and user access processes:

1. The DCT is integrated with VA's Single Sign-On External (SSOe). SSOe's identity provider is ID.me, which manages all aspects of the authentication account, including password complexity, password rotation, verification of identity, and email address.

2. The DCT authorizes ID.me accounts in the Onboarding Application based on email address to perform the initial mapping and linkage, and subsequently on the ID.me-generated "secID" value, both of which are passed as a claim in the OpenID Connect protocol.

3. Site Administrators' authorizations are kept in a local configuration file and can be changed only by editing the configuration on the host itself.

4. Site Administrators, as documented in the Standard Operating Procedure, must have valid Privileged Access as documented in EPAS. Program Administrators are authorized in the Onboarding Application by Site Administrators.

5. Applications in the DCT, such as BHL Touch and the embedded Power BI application for grantee analytics dashboard views, query the Onboarding Application user API endpoint to confirm authorization of ID.me identities.

The Contractor shall demonstrate an understanding and comprehend:

1. The system of record for Grantee Staff Users is the VA grants management system called the Universal Design Platform as a Service (UDPaaS) Grants Management System (GMS) which is expected to change in 2026 or sometime after. OSP manages entries in UDPaaS to list all users who have read/write access to the DCT.

2. Users who appear in the list with a value of "Active" are granted access to the DCT. If a user is not in the list, or has a value of anything other than Active, they are denied permission to access the DCT.

3. New Grantee Staff Users must be added to UDPaaS before they can be granted access to the DCT. Regular authorization reviews are conducted by OSP in UDPaaS, and any changes are transferred to the DCT through a bulk synchronization process (detailed in the next paragraph).

4. OPS produces a report from UDPaaS of authorized users and delivers the report to a Program Administrator, who then uploads the report to the Onboarding Application.

5. The Onboarding Application processes the report and makes changes accordingly so that the Onboarding Application and UDPaaS are in sync, either authorizing users or disabling existing users who do not appear in the list with the correct value.

    a. Completion of this step includes:

        i. Transition team access to UDPaaS user reports.

        ii. Team member authorization as a Program Administrator:

            - Uploading a UDPaaS report
            - Verifying authorization changes

5.5.2 MANAGING THE ONBOARDING APPLICATION

The Contractor shall demonstrate an understanding and ability of managing the Onboarding Application.

The key topics shall include, but not limited to:

1. **Database Schemas** – A breakdown of the data elements stored in several document-based data stores (MongoDB or DocumentDB) that support operation of the Onboarding Application, and the data analysis pipeline

2. **API Endpoints** – A comprehensive list of API endpoints offered by the Onboarding Application to effect user authorization management in the DCT, communication between the Onboarding Application and BHL Touch, and Power BI integration.

3. **Authorization Management** – An overview of the integration between VA's Identity Provider (SSOe by ID.me) and the DCT.

4. **BHL Touch Integration** – An overview of how the different components of the DCT interact with BHL Touch and for what purpose.

5. **DCT Roles and Permissions** – An overview of the three primary roles in the Onboarding Application that manage who has access to the DCT and for what purpose.

6. **Log Files** – An overview of the log files and locations used to audit activity and troubleshoot issues.

7. **Updating Policy and Procedures** – Policy and procedures for moving changes through the Development, Pre-Production, and Production environments.

5.5.3 MANAGING THE ATO PROCESS

The Contractor shall manage the ATO process.

Management of the ATO includes:

1. **Web Application Scan** – Examines web applications for common vulnerabilities and vulnerable design patterns.

2. **Penetration Scan** – Examines infrastructure for common vulnerabilities and weak communication security.

3. **Database Scan** – Examines database configurations and data management for vulnerabilities and weak protections.

4. **Controls Documentation** – Provides a comprehensive access and policy documentation managed by the ISSO and system steward in eMASS.

5. **Threat Model** – Presents a diagram-based mapping of elements, devices, and connections to identify threats.

6. **Privacy Statement** – Presents a comprehensive review of data elements, policies, and procedures of the DCT to determine privacy risk and mitigation.

5.5.4 MONITORING THE DCT AND DATA ANALYTICS PLATFORM ENVIRONMENTS

The Contractor shall monitor the DCT and Data Analytics Platform Environments.

The Contractor shall demonstrate an understanding of the transition activities related to tracking, monitoring and archiving data as well as the extracting, transforming and loading processes that are a part of the transition plan for TA and training support.

Monitoring the DCT and Data Analytics Platform Environments includes:

1. **Data Pipeline Interruptions** – Describes how to identify, and provides examples of how to triage, data pipeline issues

2. **Unexpected Data Errors Presented on the Back End** – Provides an overview of previous unexpected data errors and their resolution

3. **Infrastructure Monitoring** – Provides an overview of Dynatrace, the mandatory Tier 3 monitoring of the DCT

5.5.5 PROVIDING GRANTEE TECHNICAL ASSISTANCE FOR DCT

The Contractor shall obtain technical assistance (TA) for using the DCT from MITRE.

The Contractor shall have access to TA and training logs, and common issues that are raised by users of the DCT.
Transition for DCT TA and Training shall include:

1. **Data Collection Forms** – Overview of current data collection forms and processes

2. **Data Collection Forms Archiving** – Overview of archive process for data collection forms and previous assistance provided to grantees

5.5.6 QUALITY ASSURANCE

The Contractor shall develop a transition checklist to confirm that each activity has been performed.

The Contractor shall complete the Final Transition Handoff of Operational Tasks. This includes:

1. **Evaluating Readiness for Transition Completion** – Evaluated completion of activities in Section 5.3 through Section 5.4 of this PWS
2. **Mitigating Risks in Handoff Process** – Identifies any gaps in knowledge/skills for the new contractor prior to final handoff of the DCT platform

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

6.1.1 VA TECHNICAL REFERENCE MODEL

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

6.1.2 ZERO TRUST – VA CRITICAL SECURITY CONTROLS

VA has established minimum mandatory security requirements and requires that any network connected software system or service must meet the VA Critical Security Controls as outlined in the VA Memorandum, "VA Security Controls", https://www.voa.va.gov/DocumentView.aspx?DocumentID=5010. VA Critical Security Controls identify the minimum mandatory requirements that must be implemented across all VA enterprise infrastructure, cloud computing environments, information

systems, networks, and specialized devices (medical devices/systems, special-purpose systems, and research scientific computing devices) that process, store, and/or transmit VA data. Effective July 1, 2025, the Contractor shall implement these VA Critical Security Controls, within any network connected software system or service prior to being authorized for use in the VA. This functional requirement is not negotiable, and Plan of Action & Milestones (POAM) will not be accepted in the event these controls cannot be implemented for new systems. Critical Security Controls are intended to increase VA's security posture and provide security and privacy risk visibility into the VA network and is not a new requirement. The Contractor's failure to maintain these VA Critical Controls after implementation will result in VA discontinuing the use of the system.

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

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

The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-4, VA Handbook 6500, and VA IAM enterprise requirements for direct, assertion based authentication, and/or trust based authentication, as determined by the ETGs. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of PIV card and/or Common Access Card (CAC), as determined by the business need.

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

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

1. Automated provisioning and are able to use enterprise provisioning service.

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

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

6.1.4 INTERNET PROTOCOL VERSION 6 (IPv6)

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

(IPv6 / IPv4) users and all internal infrastructure and applications shall support using native IPv6-Only and dual stack (IPv6 / IPv4) for all functionality and operations.

6.1.5 TRUSTED INTERNET CONNECTION (TIC)

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

6.1.6 STANDARD COMPUTER CONFIGURATION

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

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

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

The VIP Guide provides guidance for transitioning from project-centric to product-centric delivery. The VIP guide applies to all OIT Office of Management and Budget (OMB)

reportable products that are required to collect and report costs, schedules, risks, and other valuable information in VA PARS (whether products are procured or developed by VA) and any VA Information Technology project effort in Software Product Management (SPM) and Infrastructure Operations (IO), or their successors, that touch the VA network regardless of IT organizational alignment (whether it spends government funding from VA's Congressional IT Appropriation or any other appropriation).

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

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

6.1.8 PROCESS ASSET LIBRARY (PAL)

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

6.1.9 AUTHORITATIVE DATA SOURCES

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

1. Interfacing with VA's Master Person Index (MPI) (formerly the Master Veteran Index (MVI)) to provision identity attributes, if the solution relies on VA user identities. MPI is the authoritative source for VA user identity data.
2. Interfacing with Capital Asset Inventory (CAI) to conduct real property record management actions, if the solution relies on real property records data. CAI is the authoritative source for VA real property record management data.

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

6.1.10 SOCIAL SECURITY NUMBER (SSN) REDUCTION

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

6.1.11 SOFTWARE AND LICENSING REQUIREMENTS

The Contractor shall be responsible for the provision of all software licenses and any associated licensing maintenance required for any development, delivery, integration,

operation, and/or maintenance associated with its proposed application(s), software products, software solution, and/or system including, but not limited to, any and all application(s), software and/or software products that comprise, are a part of, or integrate with the Contractor's proposed application(s), software products, software solution, and/or system for the life of any resulting contract.

6.1.12 GENERATIVE ARTIFICIAL INTELLIGENCE REQUIREMENTS

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

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

AI SYSTEM/LLM DEVELOPMENT AND OPERATION DOCUMENTATION REQUIREMENTS

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

1. **Acceptable Use Policy**
   The Contractor shall provide an Acceptable Use Policy document governing its AI operation that characterizes and differentiates appropriate and inappropriate use of their product offering
2. **Model Cards, System Cards and/or Data Cards**
   The Contractor shall provide documentation describing essential information about the model, system, and or data as it relates to the AI/LLM product offering. The documentation shall address summaries of training process, identified risks and mitigations, and model evaluation scores on LLM benchmarks at a minimum, where appropriate
3. **End User Resources**

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

4. **Mechanism for End User Feedback**

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

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

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

   a. Actions taken that impact the factuality and grounding of AI System/LLM outputs
   b. System-level prompts that provide natural language instructions to the model specifying guidelines on responding to user-generated queries, to include how a model responds when reliable information is incomplete, contradictory, or subject to individual interpretation
   c. The type of outputs restricted via content moderation and safety filters
   d. The use of red teaming as a means of continuously assessing the model to protect against incidents of bias in generated output.
   e. Training or development, if any, that occurred outside the United States, to include the type of activity and the country in which it occurred.
   f. Any modifications or configurations undertaken to comply with any regulation from a government other than the U.S. Federal Government.

6. **Model Evaluation Results and Methodologies**

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

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

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

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

8. **Third Party Modification Disclosure**

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

Deliverable:

A. AI System/LLM Development and Operation Documentation Package

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

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

6.2 SECURITY AND PRIVACY REQUIREMENTS

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

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

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

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.1	☒	☐	☐
5.2	☒	☐	☐
5.3	☒	☐	☐
5.4	☒	☐	☐
5.5	☒	☐	☐

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

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak, and understand the English language.
b. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the PAL template artifact. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 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 Security and

Investigations Center (SIC) 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 SIC 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 Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).

f. The Contractor employee shall certify and release the e-QIP document, print, and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM 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 e-QIP).

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 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 OPM. 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 OPM.

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. Personal Identity Verification (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

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

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

6.4 PERFORMANCE METRICS

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

Performance Objective	Performance Standard	Acceptable Levels of Performance
A. Technical / Quality of Product or Service	1. Demonstrates understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Provides quality services/products 5.	Satisfactory or higher
B. Project Milestones and Schedule	1. Established milestones and project dates are met 2. Products completed, reviewed, delivered in accordance with the established schedule 3. Notifies customer in advance of potential problems	Satisfactory or higher
C. Cost & Staffing	1. Currency of expertise and staffing levels appropriate to perform tasks required 2. Personnel possess necessary knowledge, skills, and abilities to perform tasks	Satisfactory or higher
D. Management	1. Integration and coordination of all activities to execute effort	Satisfactory or higher

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

6.5 FACILITY/RESOURCE PROVISIONS

The Government will provide office space, telephone service and system access when authorized contract staff work at a Government location as required in order to accomplish the Tasks associated with this PWS. All procedural guides, reference materials, and program documentation for the project and other Government applications will also be provided on an as-needed basis.

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

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

This remote access may provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, PAL, Primavera, and Remedy, including appropriate seat management and user licenses, depending upon the level of access granted. The Contractor shall utilize government-provided software development and test accounts, documents, and requirements repositories, etc. as required for the development, storage, maintenance, and delivery of

products within the scope of this effort. All VA sensitive information shall be protected at all times in accordance with VA Handbook 6500, local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. The Contractor shall ensure all work is performed in countries deemed not to pose a significant security risk. For detailed Security and Privacy Requirements (additional requirements of the contract consolidated into an addendum for easy reference) refer to ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED and ADDENDUM B - VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE.

6.6 SHIPMENT OF HARDWARE OR EQUIPMENT

N/A

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

Packing Slips/Labels and Lists shall also include the following:

IFCAP PO #: ____TBD_____ (e.g., 166-E11234 (the IFCAP PO number is located in block #20 of the SF 1449))
Project Description: (e.g. Tier 1 Lifecycle Refresh)

Total number of Containers: Package ___ of ___. (e.g., Package 1 of 3)

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

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

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

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

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

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

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

A2.0 VA Enterprise Architecture Compliance

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

Profile (TRMSP). VA reserves the right to assess contract deliverables for EA compliance prior to acceptance.

A2.1. VA Internet and Intranet Standards

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

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

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

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

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

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

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

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

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

☒ E208 Support Documentation and Services Requirements

A3.2. Compatibility with Assistive Technology

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

A3.3. Acceptance and Acceptance Testing

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

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

A4.0 Physical Security & Safety Requirements:

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

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

A5.0 Confidentiality and Non-Disclosure

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

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

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA CO will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA CO for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA CO.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with

published procedures to protect the privacy and confidentiality of such information as required by VA.

7. Contractor must adhere to the following:
    a. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
    b. Controlled access to system and security software and documentation.
    c. Recording, monitoring, and control of passwords and privileges.
    d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
    e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
    f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
    g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
    h. Contractor does not require access to classified data.
8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
9. VA Form 0752 shall be completed by all Contractor employees working on this contract and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

A6.0 Information Technology Using Sustainable Products and Services

Not Applicable.

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

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

APPLICABLE SECTIONS 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. The primary clause used to define computer software license (not data/intellectual property first produced under this Contractor or order) is FAR 52.227-19, Commercial Computer Software License.

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 Suitability and Security Program. The Office of Human Resources and Administration/Operations, Security and Preparedness (HRA/OSP) is responsible for these policies and procedures. Contract personnel who require access to classified information or information systems shall have an appropriate security clearance. Verification of a Security Clearance shall be processed through the Special Security Officer located in HRA/OSP. Contractors shall conform to all requirements stated in the National Industrial Security Program Operating Manual (NISPOM).

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

e. The Contractor shall notify the COR/CO in writing immediately (no later than 24 hours) after personnel separation or occurrence of other causes. Causes may include the following:
    (1) Contractor/Subcontractor personnel no longer has a need for access to VA information or VA information systems.
    (2) Contractor/Subcontractor personnel are terminated, suspended, or otherwise has their work on a VA project discontinued for any reason.
    (3) Contractor believes their own personnel or Subcontractor personnel may pose a threat to their company's working environment or to any company-owned property. This includes Contractor-owned assets, buildings, confidential data, customers, employees, networks, systems, trade secrets and/or VA data.

(4) Any previously undisclosed changes to Contractor/Subcontractor background history are brought to light, including but not limited to changes to background investigation or employee record.
(5) Contractor/Subcontractor personnel have their authorization to work in the United States revoked.
(6) Agreement by which Contractor provides products and services to VA has either been fulfilled or terminated, such that VA can cut off electronic and/or physical access for Contractor personnel.

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

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

B4. TRAINING

a. All contractors and subcontractors requiring access to VA information and VA information systems shall successfully complete the following before being granted access to VA information and its systems:
(1) VA Privacy and Information Security Awareness and Rules of Behavior course (Talent Management System (TMS) #10176) initially and annually thereafter.
(2) Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the Organizational Rules of Behavior, relating to access to VA information and information systems initially and annually thereafter; and
(3) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system or information access [to be defined by the VA program official and provided to the VA CO for inclusion in the solicitation document – i.e., any role-based information security training].

b. The Contractor shall provide to the COR/CO a copy of the training certificates and certification of signing the Organizational Rules of Behavior for each applicable employee within five days of the initiation of the contract and annually thereafter, as required.

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

B5. SECURITY INCIDENT INVESTIGATION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

B6. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

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

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

c. VA IT Contractors, Subcontractors and third-party service providers shall address and/or integrate applicable VA Handbook 6500, VA Handbook 6517, Risk Management Framework for Cloud Computing Services and Information Security Knowledge Service specifications in delivered IT systems/solutions, products and/or services. If systems/solutions, products and/or services do not directly match VA security requirements, the Contractor shall work though the COR/CO to identify the VA organization responsible for governance or resolution. Contractors shall comply with FAR 39.1, specifically the prohibitions referenced.

d. The Contractor (including producers and resellers) shall comply with Office of Management and Budget (OMB) M-22-18 and M-23-16 when using third-party software on VA information systems or otherwise affecting the VA information. This includes new software purchases and software renewals for software developed or modified by major version change after the issuance date of M-22-18 (September 14, 2022). The term “software” includes firmware, operating systems, applications and application services (e.g., cloud-based software), as well as products containing software. The Contractor shall provide a self-attestation that secure software development practices are utilized as outlined by Executive Order (EO)14028 and NIST Guidance. A third-party assessment provided by either a certified Federal Risk and Authorization Management Program (FedRAMP) Third Party Assessor Organization (3PAO) or one approved by the agency will be acceptable in lieu of a software producer's self-attestation.

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

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

g. The Contractor shall use VA authorized technical security baseline configurations and certify to the COR that applications are fully functional and operate correctly as intended on systems in compliance with VA baselines prior to acceptance or connection into an authorized VA computing environment. If the Defense Information Systems Agency (DISA) has created a Security Technical

Implementation Guide (STIG) for the technology, the Contractor may configure to comply with that STIG. If VA determines a new or updated VA configuration baseline needs to be created, the Contractor shall provide required technical support to develop the configuration settings. FAR 39.1 requires the population of operating systems and applications includes all listed on the NIST National Checklist Program Checklist Repository,

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

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

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

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

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

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

n. When the Contractor is responsible for operations or maintenance of the systems, the Contractor shall apply the security fixes within the timeframe specified by the associated controls on the VA Information Security Knowledge Service. When security fixes involve installing third party patches (such as

Microsoft OS patches or Adobe Acrobat), the Contractor shall provide written notice to the VA COR/CO that the patch has been validated as to not affecting the Systems within 10 business days.

B7. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE OR USE

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

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

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

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

e. Contractor procedures shall be subject to periodic, announced, or unannounced assessments by VA officials, the OIG or a 3PAO. The physical security aspects

associated with Contractor activities are also subject to such assessments. The Contractor shall report, in writing, any deficiencies noted during the above assessment to the VA COR/CO. The Contractor shall use VA's defined processes to document planned remedial actions that address identified deficiencies in information security policies, procedures, and practices. The Contractor shall correct security deficiencies within the timeframes specified in the VA Information Security Knowledge Service.

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

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

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

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

j. For cases wherein the Contractor discovers material defects or vulnerabilities impacting products and services they provide to VA, the Contractor shall develop

and implement policies and procedures for disclosure to VA, as well as remediation. The Contractor shall, within 30 business days of discovery, document a summary of these vulnerabilities or defects. The documentation will include a description of the potential impact of each vulnerability and material defect, compensating security controls, mitigations, recommended corrective actions, root cause analysis and/or workarounds (i.e., monitoring). Should there exist any backdoors in the products or services they provide to VA (referring to methods for bypassing computer authentication), the Contractor shall provide the VA CO/CO written assurance they have permanently remediated these backdoors.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

B10. VIRUSES, FIRMWARE, AND MALWARE

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

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

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

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

(1) Take all necessary action to correct the incident, to include any and all assistance to VA to eliminate the virus or other malware throughout VA’s information networks, computer systems and information systems; and

(2) Use commercially reasonable efforts to restore operational efficiency and remediate damages due to data loss or data integrity damage, if the virus or other malware causes a loss of operational efficiency, data loss, or damage to data integrity.

B11. CRYPTOGRAPHIC REQUIREMENT

a. The Contractor shall document how the cryptographic system supporting the Contractor's products and/or services protect the confidentiality, data integrity, authentication and non-repudiation of devices and data flows in the underlying system.

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

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

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

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

B12. PATCHING GOVERNANCE

a. The Contractor shall provide documentation detailing the patch management, vulnerability management, mitigation and update processes (to include third-party) prior to the connection of electronic devices, assets or equipment to VA's assets. This documentation will include information regarding the following:
   (1) The resources and technical capabilities to sustain the program or process (e.g., how the integrity of a patch is validated by VA); and.
   (2) The approach and capability to remediate newly reported zero-day vulnerabilities for Contractor products.

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

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

d. The Contractor shall provide or arrange for the provision of appropriate hardware, software and/or firmware updates, when those products, including open-source software, are provided to the VA, to remediate newly discovered vulnerabilities or weaknesses. Remediations of products or services provided to the VA's system environment must be provided within 30 business days of availability from the original supplier and/or patching source. Updates to remediate critical vulnerabilities applicable to the Contractor's use of the third-party product in its system environment will be provided within seven business days of availability from the original supplier and/or patching source. If applicable third-party updates cannot be integrated, tested and made available by Contractor within these time periods, mitigations and/or workarounds will be provided to the COR/CO before the above deadlines.

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

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

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

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

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

Medical Devices and Postmarket Management of Cybersecurity in Medical Devices.

e. The Contractor shall design devices capable of accepting all applicable security patches with or without the support of the Contractor personnel. If patching can only be completed by the Contractor, the Contractor shall commit the resources needed to patch all applicable devices at all VA locations. If unique patching instructions or packaging is needed, the Contractor shall provide the necessary information in conjunction with the validation/testing of the patch. The Contractor shall apply security patches within 30 business days of the patch release and have a formal tracking process for any security patches not implemented to include explanation when a device cannot be patched.

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

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

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

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

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

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

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

(b) Any fixed hard drive, Complementary Metal-Oxide-Semiconductor (CMOS), Programmable Read-Only Memory (PROM), solid state and firmware on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system

operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be pre-approved and described in the solicitation, contract, or order.

B14. DATA CENTER PROVISIONS

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.

POINTS OF CONTACT

VA Program Manager/Contracting Officer's Representative:

Name: Christian Flickinger
Voice: (318) 294-2326
Email: Christian.Flickinger@va.gov

Contracting Officer:

Name: Kimberly Geran
Address: 23 Christopher Way
Eatontown, NJ 07724
Voice: (848) 377-5228
Email: Kimberly.Geran@va.gov

ARTIFICIAL INTELLIGENCE EFFORTS

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 Package, as identified in OMB Memorandum M-26-04 as Transparency Documentation, will be provided for its proposed AI System/LLM during the period of performance, meet the required transparency threshold and align with the two Unbiased AI Principles. Failure to include the requisite Offeror's self-certification may render the Offeror's proposal/quotation unacceptable, and therefore ineligible for award. The Government will rely on the Offeror's self-certification that its proposed AI System/LLM adheres to the Unbiased AI Principles and related requirements. VA reserves the right to request additional information if it determines that doing so is in the Government's best interest.

Certification:

☒ Not Applicable.

☐ I hereby certify that the proposed AI System/LLM complies with the required Unbiased AI Principles as identified in OMB Memorandum M-26-04 and can also meet the required AI System/LLM Development and Operation Documentation requirements specified therein. I further certify that I am authorized to execute this certification on behalf of *<insert name of Offeror>*.

Printed Name of Signee: Christian Flickinger

Printed Title of Signee: Business Operations Manager

Signature: _____

Name (and version) of its proposed AI System/LLM: _____NA_____

_____

Date: _____

Company Name and Address: _____

_____

"H Clause" Incorporation
Artificial Intelligence in VA Contracts

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.

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):

https://www.acquisition.gov/far-overhaul
https://www.va.gov/oal/library/vaar/

(End of Clause)

FAR Number	Title	Date
52.203-6	RESTRICTIONS ON SUBCONTRACTOR SALES TO THE GOVERNMENT ALTERNATE I	NOV 2021
52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS	NOV 2023
52.203-19	PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS	JAN 2017
52.204-9	PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL	JAN 2011
52.204-13	SYSTEM FOR AWARD MANAGEMENT—MAINTENANCE	NOV 2025 (DEVIATION)
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	UPDATES OF PUBLICLY AVAILABLE INFORMATION REGARDING RESPONSIBILITY MATTERS	NOV 2025 (DEVIATION)
52.209-10	PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS	NOV 2025 (DEVIATION)
52.212-4	CONTRACT TERMS AND CONDITIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES	OCT 2025 (DEVIATION)
52.219-6	NOTICE OF TOTAL SMALL BUSINESS SET-ASIDE	NOV 2025 (DEVIATION)
52.219-14	LIMITATIONS ON SUBCONTRACTING	NOV 2025 (DEVIATION)
52.222-3	CONVICT LABOR	NOV 2025 (DEVIATION)
52.222-35	EQUAL OPPORTUNITY FOR VETERANS	NOV 2025 (DEVIATION)
52.222-36	EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES	NOV 2025 (DEVIATION)
52.222-37	EMPLOYMENT REPORTS ON VETERANS	NOV 2025

		(DEVIATION)
52.222-40	NOTIFICATION OF EMPLOYEE RIGHTS UNDER THE NATIONAL LABOR RELATIONS ACT	NOV 2025 (DEVIATION)
52.222-41	SERVICE CONTRACT LABOR STANDARDS	NOV 2025 (DEVIATION)
52.222-42	STATEMENT OF EQUIVALENT RATES FOR FEDERAL HIRES	MAY 2014
52.222-43	FAIR LABOR STANDARDS ACT AND SERVICE CONTRACT LABOR STANDARDS-PRICE ADJUSTMENT	NOV 2025 (DEVIATION)
52.222-50	COMBATING TRAFFICKING IN PERSONS	NOV 2025 (DEVIATION)
52.222-62	PAID SICK LEAVE UNDER EXECUTIVE ORDER 13706	NOV 2025 (DEVIATION)
52.222-90	ADDRESSING DEI DISCRIMINATION BY FEDERAL CONTRACTORS	APR 2026 (DEVIATION)
52.224-3	PRIVACY TRAINING	JAN 2017
52.226-8	ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING	MAY 2024
52.227-1	AUTHORIZATION AND CONSENT	JUN 2020
52.227-2	NOTICE AND ASSISTANCE REGARDING PATENT AND COPYRIGHT INFRINGEMENT	JUN 2020
52.227-14	RIGHTS IN DATA-GENERAL	MAY 2014
52.227-16	ADDITIONAL DATA REQUIREMENTS	JUN 1987
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
52.233-3	PROTEST AFTER AWARD	NOV 2025 (DEVIATION)
52.233-4	APPLICABLE LAW FOR BREACH OF CONTRACT CLAIM	NOV 2025 (DEVIATION)
852.201-70	CONTRACTING OFFICER'S REPRESENTATIVE	DEC 2022
852.203-70	COMMERCIAL ADVERTISING	MAY 2018
852.204-70	PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL	MAR 2026 (DEVIATION)
852.204-71	INFORMATION AND INFORMATION SYSTEMS SECURITY	FEB 2023
852.204-72	PERSONNEL VETTING AND CREDENTIALING	MAR 2026
852.215-70	SERVICE-DISABLED VETERAN-OWNED AND VETERAN-OWNED SMALL BUSINESS EVALUATION FACTORS	JAN 2023
852.215-71	EVALUATION FACTOR COMMITMENTS	OCT 2019
852.222-71	COMPLIANCE WITH EXECUTIVE ORDER 13899	APR 2025 (DEVIATION)
852.232-72	ELECTRONIC SUBMISSION OF PAYMENT REQUESTS	NOV 2018

852.239-70	SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES	FEB 2023
852.239-73	INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE	FEB 2023
852.239-74	SECURITY CONTROLS COMPLIANCE TESTING	FEB 2023
852.242-71	ADMINISTRATIVE CONTRACTING OFFICER	OCT 2020

C.2 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 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 3 years.

(End of Clause)

C.3 52.240-93 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (DEVIATION) (NOV 2025)

(a) Definitions. As used in this clause—

Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Federal contract information—

(1) Means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government; but

(2) Does not include information provided by the Government to the public (such as on public websites) or simple transactional information (such as information necessary to process payments).

Information means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

Safeguarding means measures or controls that are prescribed to protect information systems.

(b) *Safeguarding requirements*.

(1) Basic requirements. The Contractor shall safeguard its covered contractor information systems by implementing, at minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(2) Other requirements. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal departments and agencies relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(c) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial products, other than commercially available off-the-shelf items, or commercial services), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

(End of clause)

C.4 VAAR 852.239-76 INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY (FEB 2023)

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

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

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

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

(e) If this is an Indefinite-Delivery type contract, a Blanket Purchase Agreement or a Basic Ordering Agreement, the task/delivery order requests that include ICT supplies or services will define the specifications and accessibility standards for the order. In those cases, the Contractor may be required to provide a completed VA Section 508 Checklist and any other additional information necessary to assist the Government in determining that the ICT supplies or services conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies and services provided by the

Contractor do not conform to the described accessibility standards in the provided documentation, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(End of Clause)

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS

None.

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):

https://www.acquisition.gov/far-overhaul
https://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—REGISTRATION	NOV 2025 (DEVIATION)
52.212-1	INSTRUCTIONS TO OFFERORS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES	OCT 2025 (DEVIATION)
52.217-5	EVALUATION OF OPTIONS	JUL 1990
52.229-11	TAX ON CERTAIN FOREIGN PROCUREMENTS – NOTICE AND REPRESENTATION	SEP 2025 (DEVIATION)
852.233-70	PROTEST CONTENT/ALTERNATIVE DISPUTE RESOLUTION	OCT 2018
852.233-71	ALTERNATE PROTEST PROCEDURE	OCT 2018
852.239-71	INFORMATION SYSTEM SECURITY PLAN AND ACCREDITATION	FEB 2023
852.239-75	INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY NOTICE	FEB 2023

E.2 52.209-7 INFORMATION REGARDING RESPONSIBILITY MATTERS (NOV 2025) (DEVIATION)

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

Administrative proceeding means a non-judicial process that is adjudicatory in nature in order to make a determination of fault or liability (*e.g.*, Securities and Exchange

Commission Administrative Proceedings, Civilian Board of Contract Appeals Proceedings, and Armed Services Board of Contract Appeals Proceedings). This includes administrative proceedings at the Federal and State level but only in connection with performance of a Federal contract or grant. It does not include agency actions such as contract audits, site visits, corrective plans, or inspection of deliverables.

Federal contracts and grants with total value greater than $10,000,000 means—

(1) The total value of all current, active contracts and grants, including all priced options; and

(2) The total value of all current, active orders including all priced options under indefinite-delivery, indefinite-quantity, 8(a), or requirements contracts (including task and delivery and multiple-award Schedules).

Principal means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (*e.g.*, general manager; plant manager; head of a division or business segment; and similar positions).

(b) The offeror □ has □ does not have current active Federal contracts and grants with total value greater than $10,000,000.

(c) If the offeror checked "has" in paragraph (b) of this provision, the offeror represents, by submission of this offer, that the information it has entered in the Federal Awardee Performance and Integrity Information System (FAPIIS) is current, accurate, and complete as of the date of submission of this offer with regard to the following information:

(1) Whether the offeror, and/or any of its principals, has or has not, within the last five years, in connection with the award to or performance by the offeror of a Federal contract or grant, been the subject of a proceeding, at the Federal or State level that resulted in any of the following dispositions:

(i) In a criminal proceeding, a conviction.

(ii) In a civil proceeding, a finding of fault and liability that results in the payment of a monetary fine, penalty, reimbursement, restitution, or damages of $5,000 or more.

(iii) In an administrative proceeding, a finding of fault and liability that results in–

(A) The payment of a monetary fine or penalty of $5,000 or more; or

(B) The payment of a reimbursement, restitution, or damages in excess of $100,000.

(iv) In a criminal, civil, or administrative proceeding, a disposition of the matter by consent or compromise with an acknowledgment of fault by the Contractor if the proceeding could have led to any of the outcomes specified in paragraphs (c)(1)(i), (c)(1)(ii), or (c)(1)(iii) of this provision.

(2) If the offeror has been involved in the last five years in any of the occurrences listed in (c)(1) of this provision, whether the offeror has provided the requested information with regard to each occurrence.

(d) The offeror shall post the information in paragraphs (c)(1)(i) through (c)(1)(iv) of this provision in FAPIIS as required through maintaining an active registration in the System for Award Management, which can be accessed via https://www.sam.gov (see 52.204-7).

(End of provision)

E.3 52.216-1 TYPE OF CONTRACT (NOV 2025) (DEVIATION)

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

(End of Provision)

E.4 52.233-2 SERVICE OF PROTEST (SEP 2006)

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:

Hand-Carried Address:

Department of Veterans Affairs
Technology Acquisition Center
23 Christopher Way
Eatontown NJ 07724

Mailing Address:

Department of Veterans Affairs
Technology Acquisition Center
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.5 BASIS FOR AWARD

Any award will be made based on the best overall (i.e., best value) proposal that is determined to be the most beneficial to the Government, with appropriate consideration given to the five (4) following evaluation Factors: Technical Factor, Price, Past Performance and Veterans Involvement. Technical Factor One is **significantly** more important than the Price Factor, which is **slightly** more important than the Past Performance Factor, which is **slightly** more important than the Veterans Involvement Factor. To receive consideration for award, a rating of no less than "Acceptable" must

be achieved for the Technical Factor. The non-Price Factors combined are **significantly** more important than the Price Factor. Offerors are cautioned that any resulting award may not necessarily be made to the lowest price offered or the most highly rated technical proposal. The Government intends to award an FFP contract.

B. FACTORS TO BE EVALUATED

1. TECHNICAL FACTOR ONE

2. PRICE

3. PAST PERFORMANCE

4. VETERANS INVOLVEMENT

C. EVALUATION APPROACH – All proposals shall be subject to evaluation by a team of Government personnel. The Government reserves the right to award without discussions based upon the initial evaluation of proposals. The proposal will be evaluated strictly in accordance with its written and/or demonstrated content. Proposals which merely restate the requirement or state that the requirement will be met, without providing supporting rationale, are not sufficient. Offerors who fail to meet the minimum requirements of the solicitation and/or have received Unacceptable rating(s) for Past Performance will be found ineligible for award.

1. TECHNICAL EVALUATION APPROACH. The evaluation process will consider the following:

TECHNICAL FACTOR: CASE STUDIES. The Technical Factor shall evaluate the Government's confidence in the Offeror's ability, as evidenced by the past experience and expertise identified within each Case Study, as well as all artifacts provided with the Case Studies, to perform the work required in the Performance Work Statement (PWS). Although there is no specific rubric for evaluation of Case Studies, the provided artifacts will be evaluated based on how well they align with the narrative description provided for their respective case study, the technical quality of the artifact, and the appropriateness of the artifact to the functional area to which it is being proposed.

2. PRICE EVALUATION APPROACH.

Fixed Price: The Government will evaluate the price by adding the total of all line-item prices, including all options. The Total Evaluated Price will be that sum.

The Government will verify the Quoter's calculation of the total proposed price. Further, the Government may adjust the evaluated price if mathematical errors are identified. Overtime rates will not be permitted.

3. PAST PERFORMANCE EVALUATION APPROACH.

Past performance will be rated on an acceptable or unacceptable basis. The Past Performance evaluation will assess the relative risks associated with an Offeror's likelihood of success in fulfilling the solicitation's requirements as indicated by that Offeror's record of past performance.

The Government will conduct a performance risk assessment based on the quality, relevancy and recency of the Offeror's past performance as it relates to the probability of successful accomplishment of the required effort. Offerors are cautioned that the Government will review available past performance data available in the Contractor Performance Assessment Reporting System (CPARS). The Government reserves the right to obtain past performance information from any available source and may contact customers other than those identified by the Offeror when evaluating past performance. Since the Government may not necessarily interview all of the sources provided by the Offerors, it is incumbent upon the Offerors to explain the relevance of the data provided. Offerors are reminded that the burden of proving low performance risk rests with the Offerors.

The Government will review aspects of cost, schedule and performance. Areas to be evaluated may include, but are not limited to, quality of product or service, timeliness of performance or adherence to delivery schedules, and/or effectiveness in program management (to include use and control of subcontractors).

In the case of an Offeror without a record of relevant past performance or for whom information on past performance is not available, the Offeror may not be evaluated favorably or unfavorably on Past Performance.

4. VETERANS INVOLVEMENT EVALUATION APPROACH.

In accordance with Veterans Affairs Acquisition Regulation (VAAR) 852.215-70 (DEVIATION), Service-Disabled Veteran-Owned and Veteran-Owned Small Business (VOSB) Evaluation Factors, the Government will assign evaluation credit for an Offeror (prime contractor) which is a Service-Disabled Veteran-Owned Small Business (SDVOSB) or a VOSB. To receive credit, an offeror must be registered and verified in the Small Business Administration (SBA) Veteran Small Business Certification (VetCert) database at time of proposal submission and at time of award (https://veterans.certify.sba.gov/) and must meet federal small business size standards for the North American Industry Classification System (NAICS) code assigned to this solicitation.

Non-SDVOSB/VOSB Offerors proposing to use SDVOSBs or VOSBs as subcontractors will receive some consideration under this evaluation Factor. Offerors must state in their proposals the names of the SDVOSBs and VOSBs with whom they intend to subcontract and provide a brief description of the proposed subcontracts and the approximate dollar values of the proposed subcontracts. In addition, the proposed subcontractors must be registered and verified in the VetCert database (https://veterans.certify.sba.gov/) and must meet federal small business size standards for the NAICS code assigned to this solicitation at time of both proposal submission and at time of award.

E.6 SUBMISSION INSTRUCTIONS

1. INTRODUCTION

The Offeror's proposal shall be submitted electronically by the date and time indicated in the solicitation via email to Contract Specialist, Ryan.Sehulser@va.gov, and Contracting Officer, Kimberly.Geran@va.gov, in the files set forth below. The use of hyperlinks or embedded attachments in proposals is prohibited. Accordingly, any information contained within an embedded attachment and/or hyperlink will neither be accessed nor evaluated.

WARNING: Please do not wait until the last minute to submit your proposals! Late proposals will not be accepted for evaluation. To avoid submission of late proposals, we recommend the transmission of your proposal file 24 hours prior to the required proposal due date and time. Please be advised that timeliness is determined by the date and time an Offeror's proposal is received by the Government not when an Offeror attempted transmission. Offerors are encouraged to review and ensure that sufficient bandwidth is available on their end of the transmission.

2. PROPOSAL FILES. Offeror's responses shall be submitted in accordance with the following instructions:

a. Format. The submission shall be clearly indexed and logically assembled. Each volume shall be clearly identified and shall begin at the top of a page. All pages of each volume shall be appropriately numbered and identified by the complete company name, date and solicitation number in the header and/or footer. Proposal page limitations are applicable to this procurement. The Table below indicates the maximum page count (when applicable) for each volume of the Offeror's proposal.

All files will be submitted as indicated in the table below. Page size shall be no greater than 8 1/2" x 11" with printing on one side only. The top, bottom, left and right margins shall be a minimum of one inch (1") each. Font size shall be no smaller than 12-point. Arial or Times New Roman fonts are required. Characters shall be set at no less than normal spacing and 100% scale. Tables and illustrations may use a reduced font size not less than 8-point and may be landscape. Line spacing shall be set at no less than single space. Each paragraph shall be separated by at least one blank line. Page numbers, company logos and headers and footers may be within the page margins ONLY and are not bound by the 12-point font requirement. Footnotes to text shall not be used. All proprietary information shall be clearly and properly marked. If the Offeror submits annexes, documentation, attachments or the like, not specifically required by this solicitation, such will count against the Offeror's page limitations unless otherwise indicated in the specific volume instructions below. Pages in violation of these instructions, either by exceeding the margin, font, printing, or spacing restrictions or by exceeding the total page limit for a particular volume, will not be evaluated. Pages not evaluated due to violation of the margin, font or spacing restrictions will not count against the page limitations. The page count will be determined by counting the pages in the order they come up in the print layout view.

b. Content Requirements. All information shall be confined to the appropriate file. The Offeror shall confine submissions to essential matters, sufficient to define the proposal and provide an adequate basis for evaluation. Offerors are responsible for including sufficient details, in a concise manner, to permit a complete and accurate evaluation of each proposal. The titles and page limits requirements for each file are shown in the Table below:

Volume Number	Factor	File Name	Page Limitations
Volume I	Technical Factor One: Case Studies	TF1_Vendor Name.doc or docx	6 (single document, not including Artifacts or corporate affiliation for new corporate entities)
Volume II	Price	Section B Schedule of Deliverables_Vendor Name.pdf	None
Volume III	Past Performance	Past Perf_Vendor Name.pdf	None
Volume IV	Veterans Involvement	VetsI_Vendor Name.pdf	None
Volume V	Solicitation, Offer and Award Documents, Certifications and Representations	OfrRep_Vendor Name.pdf	None

A Cover Page, Table of Contents and/or a glossary of abbreviations or acronyms will not be included in the page count of the Technical Volume. However, be advised that any and all information contained within any Table of Contents and/or glossary of abbreviations or acronyms submitted with an Offeror's proposal will not be evaluated by the Government. Offerors that fail to follow the solicitation/submission instructions or submit incomplete quotations may be determined unacceptable or otherwise ineligible for award.

See also FAR 52.212-1, Instructions to Offerors – Commercial Items.

(i) VOLUME I – TECHNICAL FACTOR: CASE STUDIES.

Offerors shall submit up to two (2) relevant case studies for evaluation. Relevant case studies must demonstrate recent (within the past five (5) years immediately prior to the date of solicitation) performance of tasks detailed in the PWS, related to experience in systems configuration with an existing Commercial Off-the-Shelf (COTS) product in a Federal Cloud Enterprise, such as VA's Enterprise Cloud (PWS Section 5.3.2); experience achieving and maintaining an Authority to Operate (ATO) for a federally implemented COTS product requiring additional systems configuration, where that

product collected sensitive health information that must be protected (PWS Section 5.3.5). All case studies should describe the work performed by the Offeror in support of the 2 major functional areas detailed above.

New Corporate Entities. A new corporate entity is defined as a company that does not have recent and relevant past experience to be used for the Case Studies. New corporate entities may submit data on prior contract(s)/ order(s) involving its officers and employees, any predecessor companies, and/or corporate affiliates. Offerors that provide case studies for a corporate affiliate must include a narrative adequately describing the corporate affiliation and the anticipated meaningful participation during performance of the contract/order. However, in addition to the other requirements in this section, the Offeror shall discuss in detail the role performed by such persons or predecessor companies in the case study. Any case study cited in accordance with this section must meet the recency and relevancy requirements defined within this Volume. Additionally, any case studies cited in accordance with this Section shall include the information required for all submitted case studies.

Joint Ventures. Case Studies may be based on previous experience of any member of the Joint Venture or the Joint Venture itself. Any contracts/orders cited in accordance with this section must meet the recency and relevancy requirements defined within this Volume.

Offerors must submit Case Studies that demonstrate the two (2) relevant Functional Areas above and are strongly encouraged to submit case studies that demonstrate the capability to perform the other Functional Areas in the PWS beyond the two (2) relevant Functional Areas. Each Case Study submission is limited to three (3) pages. No more than one (1) project should be represented within a single case study.

Offerors must include the following details for each case study submission:

A. Client organization name
B. Period of performance
C. Offeror’s role for the Case Study, e.g., the prime contractor or a subcontractor
D. Background, timeline and results to include the skills, techniques and tooling used
E. Delivery methodology, e.g., prioritize rapid delivery efforts that include independent discovery of existing enterprise conventions and software engineering implementations

In addition to the above, Offerors are required to submit Artifacts to further demonstrate their capacity to perform the requirements in the PWS. Artifacts can take many formats including but not limited to text files, PDF documents, or image files. However, Artifacts are limited to human-readable data formats and artifacts submitted in machine-readable formats (e.g., CSV, JSON, XML) will not be evaluated. Artifacts must be related to the work described in one or more case studies. Artifacts may include client deliverables, code (although provided in a human-readable format), and/or screenshots. Artifacts must not be created in response to this solicitation, they must be work products generated for the described case study, however, the Offeror may transfer original artifacts to a new format for submission. For example, the Offeror may

take a screenshot of a webpage or copy site code into a text file. Multiple screenshots may be submitted as a single artifact as long as they are related to a single case study and functional area. Artifacts such as screenshots be presented in landscape. Artifacts may be anonymized as needed to protect Personally Identifiable Information, Personal Health Information, or other proprietary data, but should still demonstrate the vendor's expertise as it relates to the PWS as well as validate the past expertise detailed within the Case Study(s). Artifacts may all be from a single Case Study, or from multiple Case Studies, but there must be at least one artifact specifically related to each of the two (2) relevant Functional Areas (Offerors shall note in their Case Study submission which artifact(s) are intended to meet each of the Functional Areas), with a max of four (4) artifacts total.

The Case Studies and their respective artifacts (please include name of case study in the file name along with the name of the respective artifact and do not combine them as each one should stand alone), shall be submitted via email to Ryan.Sehulster@va.gov and Kimberly.Geran@va.gov using the instructions found above prior to the due date and time included in the solicitation. Any explanations related to the artifacts shall be included at the bottom of each case study. On a separate document please submit a list of all major subcontractors regardless of whether they have a case study attributed to them including their UEI, socio-economic size status, and the Functional Area(s) they are anticipated to support, please also include the UEI for the Prime Offeror/Joint Venture.

(ii) VOLUME II – PRICE FACTOR.

The Offeror shall complete the Section B, Schedule of Deliverables of the solicitation.

Price Rounding Issue - The Government requires Offerors to propose unit prices and total prices that are two (2) decimal places and requires the unit prices and total prices to be displayed as two (2) decimal places. Ensure that the two (2) digit unit price multiplied by the item quantity equals the two (2) digit total item price (there should be no rounding).

(ii) VOLUME III – PAST PERFORMANCE FACTOR.

Offerors shall submit a list of up to three (3) contracts (including Federal, State, and local government and private) (prime contracts, task/delivery orders, and/or major subcontracts) in performance at any point during the five (5) years immediately prior to the proposal submission date, which are relevant to the efforts required by this solicitation as indicated in the PWS. Data concerning the prime contractor shall be provided first, followed by each proposed major subcontractor, in alphabetical order. This volume shall be organized into the following sections:

(1) Section 1 – Contract Descriptions. This section shall include the following information:

(a) Contractor/Subcontractor place of performance, Commercial and Government Entity Code (CAGE) and Unique Entity Identifier (UEI) Number. If the

work was performed as a subcontractor, also provide the name of the prime contractor and Point of Contact (POC) within the prime contractor organization (name, and current address, e-mail address, and telephone and fax numbers).

(b) Contracting activity, and current address, Procuring Contracting Officer's name, e-mail address, telephone and fax numbers.

(c) Technical representative/Contracting Officer’s Representative (COR), and current e-mail address, telephone and fax numbers.

(d) Contract administration activity and the Administrative Contracting Officer's name, and current e-mail address, telephone and fax numbers.

(e) Contract Number and, in the case of Indefinite Delivery type contracts, GSA contracts, and Blanket Purchase Agreements, include Delivery Order Numbers also.

(f) Contract Type (specific type such as Fixed Price (FP), Cost Reimbursement (CR), Time & Materials (T&M), etc.) In the case of Indefinite Delivery contracts, indicate specific type (Requirements, Definite Quantity, and Indefinite Quantity) and secondary contract type (FP, CR, T&M, etc)).

(g) Awarded price/cost.

(h) Final or projected final price/cost.

(i) Original delivery schedule, including dates of start and completion of work.

(j) Final or projected final, delivery schedule, including dates of start and completion of work.

(2) Section 2 – Performance. Offerors shall provide a specific narrative explanation of each contract listed in Section 1 describing the objectives achieved and detailing how the effort is relevant to the requirements of this solicitation. For any contract(s)/task order(s) that did not/do not meet original schedule or technical performance requirements, provide a brief explanation of the reason(s) for the shortcoming(s) and any corrective action(s) taken to avoid recurrence. The Offerors shall list each time the delivery schedule was revised and provide an explanation of why the revision was necessary. The Offerors shall indicate if any of the contracts listed were terminated and the type and reasons for the termination.

(3) Section 3 – Subcontracts. Offerors shall provide an outline of how the effort required by the solicitation will be assigned for performance within the Offeror’s corporate entity and among the proposed subcontractors. The information provided for the prime Offeror and each proposed major subcontractor must include the entire company name, company address, CAGE Code, UEI Number and type of work to be performed by citing the applicable Government PWS paragraph number.

(4) Section 4 – New Corporate Entities. New corporate entities may submit data on prior contracts involving its officers and employees. However, in addition to the other requirements in this section, the Offeror shall discuss in detail the role performed by such persons in the prior contracts cited. Information should be included in the files described in the sections above.

(iv) VOLUME IV – VETERANS INVOLVEMENT FACTOR.

(1) For SDVOSBS/VOSBs: In order to receive credit under this Factor, an Offeror shall submit a statement of compliance that it qualifies as a SDVOSB or VOSB in accordance with VAAR 852.215-70, Service-Disabled Veteran-Owned and Veteran-Owned Small Business Evaluation Factors (DEVIATION). Offerors are cautioned that they must be registered and verified in the Small Business Administration (SBA) Veteran Small Business Certification (VetCert) database (https://veterans.certify.sba.gov/) and must meet federal small business size standards for the NAICS code assigned to this solicitation at time of both proposal submission and at time of award.

(2) For Non-SDVOSBs/VOSBs: To receive some consideration under this Factor, an Offeror must state in its proposal the names of SDVOSB(s) and/or VOSB(s) with whom it intends to subcontract, and provide a brief description and the approximate dollar values of the proposed subcontracts. Additionally, proposed SDVOSB/VOSB subcontractors must be registered and verified in the VetCert database (https://veterans.certify.sba.gov/) in order to receive some consideration under the Veteran's Involvement Factor and must meet federal small business size standards for the NAICS code assigned to this solicitation at time of proposal submission and time of award.

(v) VOLUME V - SOLICITATION, OFFER AND AWARD DOCUMENTS AND CERTIFICATIONS/REPRESENTATIONS.

Certifications and Representations - An authorized official of the firm shall sign the SF 1449 and all certifications requiring original signature. An Acrobat PDF file shall be created to capture the signatures for submission. This Volume shall contain the following:

a. Solicitation Section A – Standard Form (SF1449) and Acknowledgement of Amendments, if any.

b. Any proposed terms and conditions and/or assumptions upon which the proposal is predicated.

Offerors are hereby advised that any Offeror-imposed terms and conditions and/or assumptions which deviate from the Government's material terms and conditions established by the Solicitation, may render the Offeror's proposal Unacceptable, and thus ineligible for award.